الجرائم الالكترونية
و الوقاية منها
فى القانون الجزائرى

فى ضوء

الإتفاقية العربية لمكافحة جرائم تقنية المعلومات
قانون العقوبات - قانون الإجراءات الجزائية
قوانين خاصة



دكتور
يزيد بوحليط
كلية الحقوق و العلوم السياسية
جامعة 8 ماى 1945 قالمة
الجزائر



الجرائم الالكترونية
والوقاية منها فى القانون الجزائرى

فى ضوء :

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

قانون العقوبات – قانون الاجراءات الجزائية

قوانين خاصة

دكتور

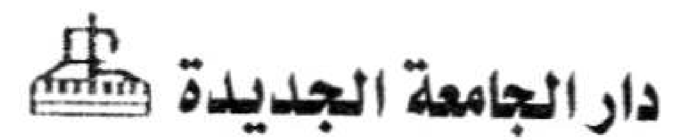
يـزيـد بـوحـليـط

كلية الحقوق والعلوم السياسية

جامعة 8 ماى 1945 قالمة

الجزائر

2019



دار الجامعة الجديدة

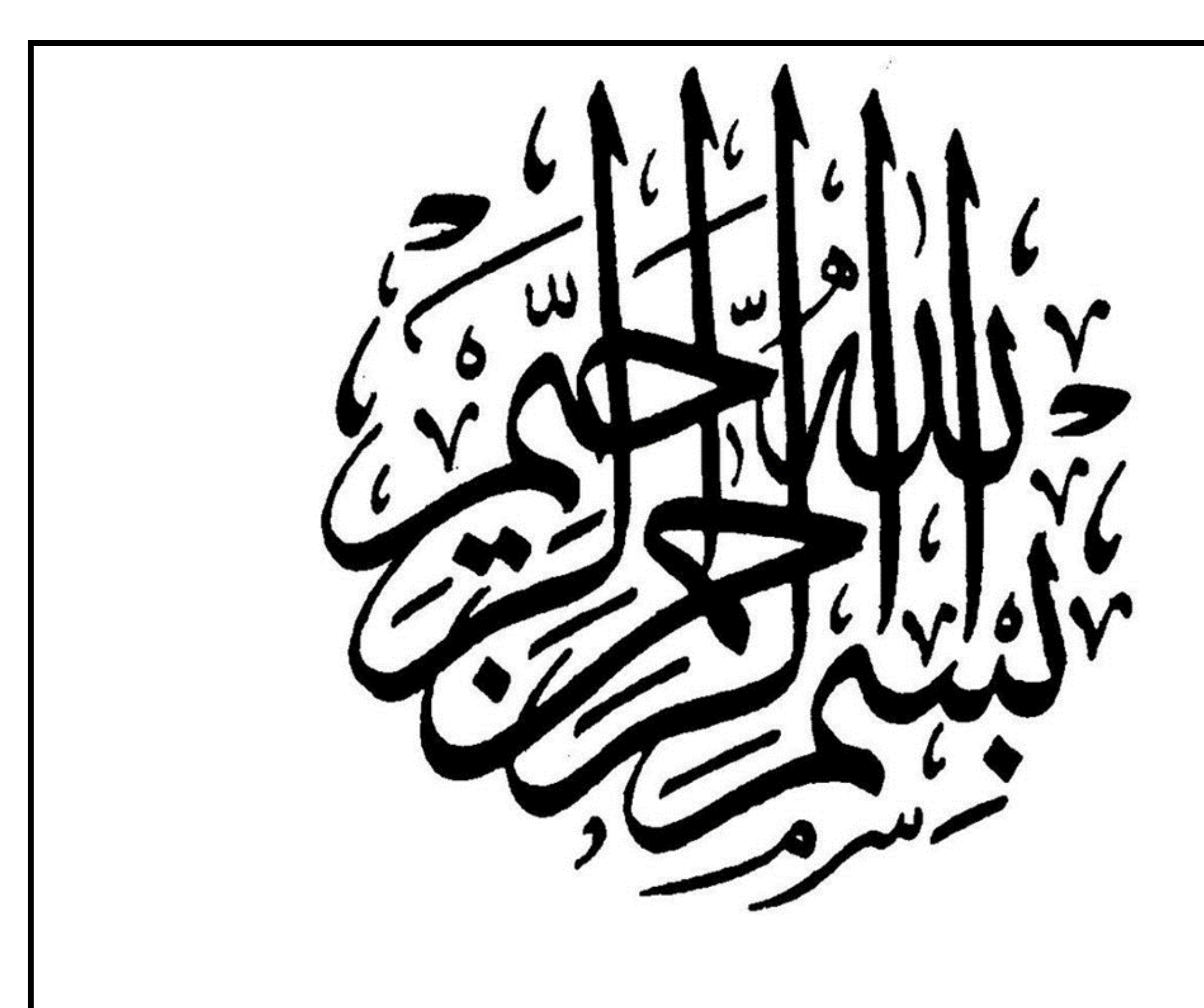
٣٨–٤٠ ش سـوتير – الأزاريطة – الإسـكندرية

تليفون: ٤٨٦٣٦٢٩ فاكس: ٤٨٥١١٤٣ تليفاكس: ٤٨٦٨٠٩٩

E-mail: darelgamaaelgadida@hotmail.com

info@darggalex.com www.darggalex.com

رقم الإيداع	2018/25535
الترقيم الدولى	I.S.B.N
978-977-729-515-4	


بسم الله الرحمن الرحيم


بسم الله الرحمن الرحيم

شكـــر

أحمد الله تعالى العلي القدير، أن وفقني وأعانني على إتمام هذا العمل من غير حول مني ولا قوّة ، فهو الذي له الفضل أولا وأخيرا ، فللّه الحمد والمنّة...

المؤلف: د. يزيد بوحليط

جامعة 8 ماي 1945 قالمة

مخبر الدراسات القانونية البيئية

البريد المهني: bouhalit.yazid@univ-guelma.dz

2019

قائمة المختصرات.

- (ق.ع.ج) : قانون العقوبات الجزائري.
- (ق.إ.ج.ج) : قانون الإجراءات الجزائية الجزائري.
- (ق.م.ج) : القانون المدني الجزائري.

- (ق.إ.م.إ.ج): قانون الإجراءات المدنية والإدارية الجزائري.
- (ق.ت.ج) : القانون التجاري الجزائري.
- (ق.ع.ف) : قانون العقوبات الفرنسي.
- (ق.إ.ج.ف): قانون الإجراءات الجنائية الفرنسي.
- (إ.ع.م.ج.ت.م) : الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
- (إ.أ.م.إ.م) : الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي.
- (ج. ر) : الجريدة الرسمية.
- (ط): الطبعة.
- (ج): الجزء.
- (ب.س.ط): بدون سنة الطبع.
- (ب. د. ن): بدون دار النشر.
- (.../...): المادة/الفقرة.
- (...–...): المادة...إلى المادة...

مقدمة

بدأت الثورة المعلوماتية نتيجة التزاوج بين تقنية الحوسبة من جهة، وتقنية الاتصال من جهة أخرى، فالثورة المعلوماتية هي الطفرة العلمية والتكنولوجية التي نشهدها اليوم، حتى بات يطلق على هذا العصر بعصر المعلومات، حيث صار العالم عبارة عن قرية صغيرة لا اعتراف فيها بالحدود الجغرافية، يتواصل الناس فيما بينهم بكل يسر. وتعدُّ المعلومة أهم ممتلكات الإنسان، التي اهتم بها على مرّ العصور فجمعها ودوّنها وسجّلها على وسائط عديدة، بدأت بجدران المعابد، ثم انتهت باختراع الورق الذي تعددت أشكاله، حتى وصل الأمر إلى استعمال وسائط التخزين الإلكترونية كالأشرطة المغناطيسية والأقراص المضغوطة.

وعليه تتجسّد تقنية المعلومات أساسا، في الانتشار الواسع لشبكة الإنترنت وأجهزة الحاسوب التي تتطور بشكل مستمر، وتستعمل برامج متقدمة وشبكات اتصال محلية أو عالمية، حيث لا نكاد نستغني يوميا عن هذه التقنية في تسيير شتى مجالات حياتنا، حيث أتاح الفضاء السيبيري الاتصال المستمر بين الدول، وأصبحت شبكة الإنترنت اليوم تشهد حضورا قويا في جميع المجالات العلمية والبحثية والاقتصادية والسياسية والاجتماعية على السواء. من جهة أخرى مكّنت تقنية المعلومات من تطوير أنظمة المعلومات بهدف الاطلاع على المعلومات وتبادلها ومعالجتها آليا بواسطة الحاسوب وشبكة الإنترنت. حيث فتحت مجالات واسعة أمام الدول للمضي قُدما في تجسيد متطلبات الحكومة الإلكترونية والاعتماد على التجارة الإلكترونية مثل: استعمال وسائل الدفع الإلكتروني والنقود الإلكترونية والبنوك الإلكترونية...إلخ.

لكن بالمقابل أدى سوء استخدام هذا الفضاء الافتراضي إلى بروز نوع جديد من الجرائم المستحدثة، لم يكن للإنسان سابق عهد بها أُصطلح على تسميتها: "بالجرائم الإلكترونية" أو "الجرائم المعلوماتية" تتميز بخصائص فريدة من نوعها وذات طبيعة خاصة، تختلف في مفهومها وأركانها ووسائل ارتكابها ونوعية الجناة والمجنى عليهم فيها عن الجرائم التقليدية المعروفة، مما خلق صعوبات بالغة لأجهزة البحث والتحريّ لملاحقة المجرم الإلكتروني وتوقيع العقاب عليه.

أهمية الموضوع:

تعتبر الجريمة ظاهرة اجتماعية تتأثر طبيعتها وحجمها بالتحولات التقنية والإقتصادية والإجتماعية والثقافية دوليا ووطنيا. وعليه فإنّ ثورة تقنية المعلومات صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة، نتيجة سوء استخدامها والانحراف عن الأغراض المتوخاة منها، حيث ازدادت هذه المخاطر تفاقماً في ظلّ البيئة الافتراضية التي تمثلها شبكة الإنترنت واسعة الانتشار

حيث ظهر للوجود نمط جديد من الجرائم المستحدثة ذات طبيعة خاصة تختلف عن الجرائم التقليدية تتسبب في أضرار نفسية واجتماعية واقتصادية كبيرة. حيث تتم في بيئة افتراضية عابرة للحدود مما يصعُب اكتشافها وإثباتها.

وعليه تتعرض المصالح التقليدية التي تحميها كل التشريعات والنظم القانونية منذ زمن إلى أشكال مستحدثة من الاعتداء بواسطة هذه التقنية الحديثة، فبعد أن كان الاعتداء على الأموال يتم بواسطة السرقة التقليدية أو النصب، أصبحت هذه الأموال يُعتدي عليها عن طريق اختراق الشبكات المعلوماتية وإجراء التحويلات الإلكترونية في لحظات معدودة، كما يتم الاعتداء على الحقوق الثابتة في الأوعية الورقية عن طريق اختراق الشبكات والأنظمة المعلوماتية، دون الحاجة إّلى المساس بأيّ وثائق أو مُحرّرات ورقية، إضافة إلى قرصنة المواقع الإلكترونية وأنظمة المعالجة الآلية للمعطيات وقواعد البيانات سواء المتعلقة بالأفراد أو مؤسسات الدولة، إضافة إلى الاعتداءات الماسة بحرمة الحياة الخاصة التي تستعمل فيها تكنولوجيات الإعلام والاتصال. مما خلق صعوبات بالغة في تعامل المشرّع معها، سواء في الجانب الموضوعي المتعلق بالتجريم والعقاب أو في الجانب الإجرائي المتعلق بالبحث والتحرّي للكشف عن الجريمة واستخلاص الدليل الرقمي لإدانة المجرم.

من جهة أخرى، تسعى الجزائر ككل الدول إلى الاستفادة من تكنولوجيات الإعلام والاتصال والعمل على الانتشار الواسع لاستعمال الحاسوب وشبكة الإنترنت في شتى المجالات، وهو ما يترجم اتجاه الجزائر نحو توفير متطلبات الحكومة الإلكترونية والتجارة الإلكترونية، رغم ما يفرضه ذلك من تحديات كبيرة لتأمين هذا الفضاء من مختلف أشكال الجرائم الإلكترونية.

وإدراكا من المشرع الجزائري بخطورة الجرائم الإلكترونية على كافة الصُعُد، وتماشيا مع الاتجاه العالمي لمكافحة هذا النوع المستحدث من الجرائم، قام بالنصّ على تجريم الاعتداءات الواقعة ضد الأشخاص باستعمال تكنولوجيا الإعلام والاتصال، مثل: جرائم الإهانة أو السبّ أو القذف باستعمال الوسائل الإلكترونية أو المعلوماتية وعموما بأيّ وسيلة إلكترونية توفّرها التقنية الحديثة بموجب المواد:(144مكرر) و(144مكرر2) و(146) من قانون العقوبات. كما نصّت المواد من (303مكرر-303مكرر3) من قانون العقوبات على جرائم المساس بحرمة الحياة الخاصة للأفراد باستعمال الوسائل التقنية.

وفي الصدد نفسه، قام المشرّع بتعديل قانون العقوبات بموجب القانون رقم:04-15 المؤرخ في:10 نوفمبر2004، بإضافة قسم سابع مكرّر عنوانه" جرائم المساس بأنظمة المعالجة الآلية للمعطيات" من المواد: (394 مكرر إلى 394 مكرر7)، وهي خطوة هامة على مسار مكافحة الجرائم الإلكترونية. ونظرا لعدم كفاية الإجراءات التقليدية في مجال البحث والتحرّي عن الجرائم الإلكترونية

قام المشرّع بتعديل قانون الإجراءات الجزائية بموجب القانون رقم:06-22 المؤرخ في 2006/12/20 المعدّل والمتمم لقانون الإجراءات الجزائية، أين نصّ على أساليب خاصة للبحث والتحريّ، تتناسب والطبيعة الخاصة للجرائم الإلكترونية، مثل: اعتراض المراسلات وتسجيل الأصوات والتقاط الصوّر والتسرّب، وذلك بموجب المواد:(65 مكرر5 إلى 65 مكرر18).

ونظرا للخطورة البالغة التي تمثلها الجرائم الإلكترونية على مختلف المصالح المحمية قانونا، لم يقف المشرّع عند تجريم الفعل بعد حدوثه، ولكن امتدّ ذلك إلى ما قبل وقوعه بهدف الوقاية منه، وذلك حينما نصّ في القانون رقم: 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على جملة من الإجراءات الوقائية الخاصة بمكافحة هذه الجرائم، مثل: المراقبة الإلكترونية وإجراء تفتيش المنظومة المعلوماتية وحجز المعطيات واعتراض المراسلات، والتعاون القضائي والمساعدة الدولية المتبادلة...إلخ، إضافة إلى التصديق بتاريخ:2014/09/28 على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة في:2010/12/21 والتي تُمثّل البعد الدولي للمشرّع لمكافحة هذه الجرائم، حيث نصّت هذه الاتفاقية على جملة من الجرائم الإلكترونية لازال المشرّع لم يجرّم بعضها. من جانب آخر اتجه المشرع إلى تجريم بعض أشكال الجرائم الإلكترونية ضمن نصوص خاصة، كقانون التأمينات الاجتماعية، وقانون التوقيع والتصديق الإلكترونيين، وهو ما يترجم السياسة الجنائية الشاملة في شقيّها الموضوعي والإجرائي للمشرع بخصوص اعتماد مكافحة فعّالة هذه الجرائم المستحدثة.

وتجدر بنا الإشارة إلى أنّنا سنتعرض للجرائم الإلكترونية بمفهومها الواسع، والذي يدخل تحته كافة الجرائم، التي تتم باستعمال تكنولوجيات الإعلام والاتصال، وعموما بأيّ وسيلة إلكترونية كانت. إذ سنتناول وبصفة موجزة كلّ جريمة على حدة مع تبيان أركانها والعقوبات المقررة لها، بموجب قانون العقوبات أو بموجب نصوص خاصة أو بموجب الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. إضافة إلى توضيح كافة الإجراءات المستحدثة بموجب قانون الإجراءات الجزائية، والتي أقرّها المشرّع للسلطات المكلفة بالتحقيقات والتحرّيات في مجال الكشف عن الجريمة وملاحقة مرتكبيها.

دوافع اختيار الموضوع:

أدى التطور المستمر في صناعة الحوسبة والاتصال إلى انتشار التقنية المعلوماتية في شتى مجالات الحياة. فأصبح من السهل الآن اقتناء جهاز حاسوب أو هاتف نقّال، مزودين بخدمة النفاذ لشبكة الإنترنت، بما يقدم خدمات عديدة، توفيرا للجهد والمال والوقت، لكن بالمقابل أدى سوء استخدام هذه التقنية إلى ظهور جرائم مستحدثة، كجرائم المساس بأنظمة المعالجة الآلية للمعطيات وجرائم الاعتداء على حرمة الحياة الخاصة وغيرها، وما يتركه ذلك من آثار سلبية على الفرد والمجتمع، ومن

باب اهتمامنا وشغفنا بهذه التقنية، أردنا البحث في هذا الموضوع من جهة، للتعرّف على الجرائم المرتكبة في هذا المجال، لأنّها حتما تختلف في طبيعتها عن الجرائم التقليدية المعروفة، خاصة في ظل انتشار تكنولوجيات الإعلام والاتصال والارتفاع المتزايد لمستعملي شبكة الانترنيت في الجزائر ومن جهة أخرى، معرفة السياسة الجنائية للمشرع الجزائري في شقّيها الموضوعي والإجرائي بخصوص مكافحة هذا النوع المستحدث من الجرائم.

الإشكالية:

تُخلّف الجرائم الإلكترونية آثارا مُدمرة على المستوى النفسي والاجتماعي والاقتصادي للدولة خاصة في ظل التقدّم المذهل للتقنية المعلوماتية، ولم يُعد خطرها أو آثارها محصورة في النطاق الإقليمي لدولة بعينها، الأمر الذي بات يثير كثيرا من التحديات القانونية والعملية أمام الأجهزة القضائية المكلفة بالبحث والتحرّي عن هذه الجرائم، وبالذات فيما يخصّ كشفها وإثباتها، وإجراءات مباشرة البحث والتحرّي واستخلاص الأدلّة الرقمية عبر هذه البيئة الافتراضية لتعقّب المجرم المعلوماتي وتقديمه للعدالة. وأمام هذا التحدّيات كان لزاما على المشرّع الجزائري التدخل دون تمهُّل لوضع حدّ لها، عن طريق تعديل أو استحداث نصوص قانونية، تتلاءم وطبيعة هذه الجرائم الجديدة. وسواء كان هذا التدخل بتعديل قانون العقوبات أو بتعديل قانون الإجراءات الجزائية أو بموجب قوانين خاصة، أو عن طريق التصديق على الاتفاقيات الدولية أو إبرام اتفاقيات ثنائية بخصوص المساعدة القضائية المتبادلة في هذا المجال.

وعليه يمكن طرح الإشكالية الآتية:

ما مدى فعالية السياسة الجنائية بشقيّها الموضوعي والإجرائي لمواجهة الجرائم الإلكترونية في التشريع الجزائري؟.

أهداف البحث:

تتلخص أهداف البحث في النقاط الآتية:

- التعرّف على الجوانب الموضوعية المتعلقة بالتجريم والعقاب في التشريع الجزائري الخاصة بمكافحة الجرائم الإلكترونية بمفهومها الواسع ضمن إطار قانون العقوبات وبعض القوانين الخاصة.
- التعرف على الجوانب الإجرائية المتعلقة بهذا النوع المستحدث من الجرائم، مرورا بكافة مراحل الدعوى وانتهاء بالتعاون القضائي والمساعدة القضائية الدولية في هذا الشأن.
- مدى كفاية وفعالية النصوص القانونية في مواجهة الجرائم الإلكترونية، خاصة في ظل التطور المستمر لتكنولوجيات الإعلام والاتصال.

المنهج المتبع:

استعملنا في دراستنا هذه منهج تحليل المحتوى، بقصد تحليل مضمون النصوص القانونية المتضمنة الجرائم الإلكترونية محلّ الدراسة واستنباط الأحكام المتعلقة بها. كما استخدمنا أيضا المنهج المقارن، لمعرفة موقف المشرّع الجزائري في بعض المسائل مقارنة مع التشريعات الأخرى، وذلك للاستفادة من تجارب الدول الأخرى وفهم النصوص القانونية وتطبيقاتها.

الدراسات السابقة:

يعتبر هذا الموضوع من الموضوعات الحديثة، نتج عنه وجود دراسات قليلة تناولت بعض جوانبه، نذكر منها:

– محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية–دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، قسم القانون الخاص، جامعة باجي مختار، عنابة، الجزائر، 2011 .

تطرق فيها إلى النظام القانوني، الذي يحكم جريمة التواجد غير المشروع في الأنظمة المعلوماتية والجرائم المرتبطة بها، وما مدى نجاعة الحماية الجنائية للحدّ من هذه الجريمة، وذلك في التشريع الجزائري وبعض التشريعات الأخرى. حيث تمثل هذه الجريمة إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات، التي نصّ عليها المشرع بموجب القانون رقم: 04-15 المعدل والمتمّم لقانون العقوبات، مما يستوجب من جهة تسليط الضوء على الجرائم الأخرى المتبقية ضمن الجرائم الواقعة على المنظومة المعلوماتية، ومن جهة أخرى التطرق إلى الجرائم الإلكترونية اعتمادا على المفهوم الموسّع لها.

– فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه كلية الحقوق جامعة الجزائر 1، الجزائر، 2011.

تناول فيها عرض النصوص القانونية التقليدية المتعلقة بالجانب الموضوعي والإجرائي ومدى كفايتها في موجهة الجرائم المعلوماتية سواء في القانون الجزائري أو اليمني، ثم تطرق إلى النصوص القانونية المستحدثة في كلا القانونين لمواجهة الجريمة المعلوماتية، وهل مكّنت هذه النصوص مكافحة فعالة تتلاءم وطبيعة هذه الجرائم. مما يجعلنا نُتم بحثه في هذا المجال، بالتطرّق إلى النصوص القانونية الجديدة الصادرة بعد سنة 2011، لمعرفة تطور جهود المشرع الجزائري في مكافحة هذه الجرائم.

– عبد العزيز نويري، الحماية الجزائية للحياة الخاصة، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر،2011.

تطرّق فيها إلى الحماية الجزائية للخصوصية الفردية ضمن التشريع الجزائري وبعض التشريعات المقارنة، ومدى فعاليتها واقعيا للحفاظ عليها من كافة أشكال الاعتداءات الحديثة، مثل: إجراء تسجيل الأصوات والتقاط الصور...إلخ.

– فضيلة عاقلي، الحماية القانونية للحق في حرمة الحياة الخاصة، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2012.

تطرّقت فيها إلى الحماية الجزائية لحرمة الحياة الخاصة في ظل تقنية المعلومات، وما توفره هذه التكنولوجيا من وسائل يمكن من خلالها المساس بها. وهل تدخل المشرّع بالقدر المناسب لحمايتها.

– صبرينة بن سعيد، حماية الحق في حرمة الحياة الخاصة في عهد تكنولوجيا الإعلام والاتصال، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر 2015، ص198.

تطرّقت فيها إلى انعكاس تكنولوجيات الإعلام والاتصال على الحق في حرمة الحياة الخاصة والتهديدات المحتملة له، وهل تمكّن المشرّع الجزائري في منظومته القانونية توفير القدر اللاّزم من الحماية لها في ظلّ ما يشهده العالم من تطور مستمر لتقنية المعلومات.

الصعوبات المعترضة للبحث:

نلخصها فيما يأتي:

– طبيعة الموضوع وحداثته: تعتبر طبيعة الموضوع من الصعوبات التي واجهت الباحث فإذا كانت الدراسة قانونية، فإن لهذا الموضوع طبيعة تقنية بحتة لا غنى للباحث عن فهمها وتناولها فارتباط الجرائم محلّ الدراسة بالتقنية الحديثة في مجال الحاسوب والأنظمة المعلوماتية وشبكة الإنترنت وتكنولوجيات الإعلام والاتصال عموما، يحتاج من الباحث بذل جهد إضافي لفهم هذه الجوانب التقنية والتي ستقوده حتما إلى فهم أفضل للجوانب القانونية.

– نقص المراجع: مثّل نقص المراجع هاجسا كبيرا للباحث، خاصة المراجع المتخصصة منها فضلا عن قلّة المراجع الجزائرية في هذا المجال، لأن الدراسة ضمن التشريع الجزائري.

– نقص التطبيقات القضائية المتعلقة بموضوع الدراسة: لعبت حداثة النصوص التشريعية المتعلقة بموضوع البحث، دورا بارزا في قلّة الأحكام القضائية في هذا الشأن.

– قلّة الإحصائيات الرسمية حول انتشار الجرائم الإلكترونية في الجزائر، من حيث عددُها ومجالات ارتكابها والأضرار المترتبة عنها.

التصريح بالخطة:

قصد إعطاء صورة واضحة عن أبعاد السياسة الجنائية للمشرع الجزائري بخصوص مكافحة الجرائم الإلكترونية، وما يثير ذلك من إشكالات في الجانبين الموضوعي والإجرائي، ارتأينا تقسيم بحثنا هذا إلى بابين:

– الباب الأول عنوانه: الأحكام الموضوعية في مكافحة الجرائم الإلكترونية، حيث قسّمناه إلى فصلين، نتناول في الفصل الأول: ماهية الجرائم الإلكترونية، ثم نتطرق في الفصل الثاني إلى الجوانب الموضوعية للجرائم الإلكترونية، وهذا بموجب قانون العقوبات وبعض النصوص الخاصة إضافة إلى بعض نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

– الباب الثاني: تحت عنوان: الأحكام الإجرائية في مكافحة الجرائم الإلكترونية، حيث قسّمناه إلى فصلين، نتناول في الفصل الأول: إجراءات جمع الدليل الإلكتروني وحجيته في الإثبات الجنائي، ثم نتطرق في الفصل الثاني إلى: القواعد الخاصة للوقاية من الجرائم الإلكترونية بموجب القانون رقم: 09-04 المؤرخ في:05 غشت سنة2005 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إضافة إلى التطرّق لبعض الصعوبات الموضوعية والإجرائية التي تواجه سلطات البحث والتحرّي باعتبارها الواجهة الأولى لمكافحة هذا النوع المستحدث من الجرائم.

وأنهينا بحثنا بخاتمة ضمنّاها أهم النتائج والتوصيات المقترحة.

الباب الأول: الأحكام الموضوعية في مكافحة الجرائم الإلكترونية

أدى التقدم التكنولوجي الهائل في مجال تكنولوجيات الإعلام والاتصال إلى انتشار هذه التقنية في كافة نواحي الحياة، حتى أصبح لا غنى للإنسان عنها، لكن بالمقابل نتج عن إساءة استخدامها

جرائم مستحدثة تختلف في مفهومها وأركانها وطرق وأدوات ارتكابها، ونوعية الجناة والمجنى عليهم فيها عن الجرائم التقليدية المعروفة، فهي تخلف أضرارا بالغة وخسائر كبيرة على مستويات عدة، سواء بالنسبة للحكومات أو للمؤسسات والشركات أو للأفراد. فمثلا تكلّف هذه الجرائم الاقتصاد الأمريكي ما يقارب 250 مليار دولار سنويا، أي ما يعادل ميزانيات أغلب دول العالم الثالث تقريبا[1]. من جانب آخر، خلق هذا النوع المستحدث من الجرائم صعوبات بالغة سواء على مستوى التجريم والعقاب أو على مستوى الإجراءات المتعلقة بالبحث والتحري عنها.

ولذلك ارتأينا أن نقسم هذا الباب إلى فصلين: نلقي الضوء على ماهية الجرائم الإلكترونية في(الفصل الأول)، ثم نتطرق إلى الجوانب الموضوعية للجرائم الإلكترونية التي تمثل مجمل النصوص القانونية المتعلقة بمكافحتها في (الفصل الثاني).

الفصل الأول: ماهية الجرائم الإلكترونية

لا يمكن للمشرع في سياسته الجنائية، أن يضع الأحكام الموضوعية المتعلقة بالتجريم والعقاب بخصوص الجرائم الإلكترونية، ما لم يدرسها ويفهمها جيدا من جوانب مختلفة، قصد تحديد مفهومها وأركانها وأساليب ارتكابها...إلخ، وقصد الإلمام بماهية الجرائم الإلكترونية أو (المعلوماتية)، قسمنا هذا الفصل إلى ثلاثة مباحث، سنتطرق إلى مفهوم الحاسوب وشبكة الإنترنت وتطورهما في (المبحث الأول)، ثم نوضح مفهوم الجريمة الإلكترونية في (المبحث الثاني)، وأخيرا نتطرق إلى البنيان القانوني لها في (المبحث الثالث).

المبحث الأول: مفهوم الحاسوب وشبكة الإنترنت

إن دراسة السياسة الجنائية للمشرع الجزائري في مجال مكافحة الجرائم الإلكترونية، يتطلب منّا التطرق أولا إلى تعريف الحاسوب وشبكة الإنترنت في جوانبهما الفنية والتقنية وكيفية عملهما، وكذا تطورهما التاريخي في(المطلب الأول)، ثم نتناول دور الحاسوب في مجال ارتكاب الجريمة الإلكترونية في (المطلب الثاني)، إضافة إلى الحديث عن دوافع المجرم الإلكتروني في ارتكاب جريمته في(المطلب الثالث) لنختم في الأخير بعرض الأضرار الاقتصادية والنفسية والاجتماعية المتنوعة التي يخلفها هذا النوع المستحدث من الجرائم في (المطلب الرابع).

المطلب الأول: تعريف الحاسوب وشبكة الإنترنت وتطورهما التاريخي

[1] عماد مجدي عبد الملك، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2011، ص28.

يمثل الحاسوب وشبكة الإنترنت أهمية بالغة في شتى مجالات حياتنا، نظرا للخدمات الكثيرة التي يقدمانها، لذلك سنتطرق لتعريف الحاسوب وتطوره التاريخي في (الفرع الأول)، ثم نتناول تعريف شبكة الإنترنت وتطورها التاريخي في (الفرع الثاني).

الفرع الأول: تعريف الحاسوب وتطوره التاريخي:

أحدثت الثورة التكنولوجية الحديثة قفزة هائلة في مجال صناعة تكنولوجيات الإعلام والاتصال تمثّلت أساسا في انتشار استعمال الحاسوب على كافة الصُعد، خاصة في ظل وجود شبكة الإنترنت التي جعلت من العالم قرية صغيرة، أتاحت فرصا جديدة للاطلاع على المعلومات وتبادلها بين ملايين البشر وبضغطة زر.

أولا: تعريف الحاسوب: لا يخفى على أحد اليوم أهمية المعلوماتية *(informatique)* في حياتنا اليومية فهي:" علم المعالجة العقلانية بواسطة الحاسب الآلي للمعلومات التي تعتبر دعامة للمعارف الإنسانية في مجال التقنية والاتصالات"[1]. وعليه هناك عدة تعاريف للحاسوب[2] نذكر بعضها: فهو عبارة عن: "مجموعة من الأجهزة متكاملة مع بعضها البعض، بهدف تشغيل مجموعة من البيانات الداخلة وفقا لبرنامج موضوع مسبقا للحصول على النتائج المطلوبة"[3]، أو هو:" جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات وذلك باستقبال المدخلات ومعالجتها وإظهار النتائج"[4]، أو هو: "آلة إلكترونية تتخذ القرارات المنطقية على البيانات الرقمية بوسائل إلكترونية باستعمال البرامج المخزنة فيه"[5]، وعرّفه آخرون على أنه: "مجموعة متكاملة من الأجهزة التي تعمل معا بهدف تشغيل*(process)* مجموعة البيانات الداخلة *(input data)* طبقا لبرنامج *(program)* تم وضعه مسبقا للحصول على نتائج معينة"[6]، كما عرفه

---

[1] *André Lucas et Jean Devèze et Jean Frayssinet, Droit de L'informatique et de L'internet, Presse Universitaire de France, 2001,p.05.*

[2] الحاسوب أو الحاسب هي الترجمة التي استخدمها مجمع اللغة العربية للكلمة الإنجليزية *(Computer)*، وما يقابلها باللغة الفرنسية *(Ordinateur)*، كما تجدر الإشارة إلى أن الجيل الحالي للحاسبات يعمل بواسطة الذكاء الاصطناعي، وبالتالي لا حاجة لاستخدام كلمة(آلي) بعد كلمة حاسوب. راجع، نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع عمان، الأردن، ط1، 2008، ص20.

[3] محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر،2003، ص13.

[4] نهلا عبد القادر المومني، المرجع السابق ، ص20.

[5] جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع عمان، الأردن، ط1 2010، ص24.

[6] عبد العال الديربي ومحمد صادق اسماعيل، الجرائم الإلكترونية-دراسة قانونية قضائية مقارنة، المركز القومي للإصدارات القانونية القاهرة، مصر، ط1، 2012، ص16.

القانون الأمريكي بأنه: "جهاز إلكتروني بصري كيميائي كهربائي ذو سرعة عالية، يؤدي وظائف منطقية حسابية أو تخزينية ويشتمل على أي جهاز لتسهيل تخزين المعلومات أو تسهيل اتصالات مباشرة مقترنة أو تعمل بالاقتران مع هذا الجهاز"[1].

نستنتج من التعاريف السابقة، أن الحاسوب يتألف من مكونات مادية وأخرى معنوية، فما المقصود بهما؟.

أ- **المكونات المادية للحاسوب*(Hardware)***: يقصد بالمكونات المادية للحاسوب:" الأشياء الملوسة من أجزائه وأدواته التي تعمل بشكل متكامل لأداء مهمة في معالجة البيانات آليا"[2]. وعليه يتكون الحاسوب من عدة وحدات مثل: وحدات الإدخال *(Input Units)* كلوحة المفاتيح وشاشات اللّمس ونظام الإدخال المرئي والصوتي، إضافة إلى وحدة الذاكرة الرئيسية *(Main Memory)*التي تستخدم في الحفظ الدائم أو المؤقت للبيانات والمعلومات والبرامج، وأيضا وحدة التحكم أو وحدة المعالجة المركزية *(Central Processing Unit)* التي تقوم بالتنسيق بين الوحدات الأخرى وضبط التعليمات، إضافة لوسائط إظهار نتائج التشغيل ومعالجة البيانات *(Output Units)* كالشاشة والطابعة والراسم، إضافة إلى الأقراص المرنة والصلبة التي تعتبر من أشهر دعائم تخزين البيانات و المحافظة عليها[3].

ب- **المكونات المعنوية(المنطقية) للحاسوب*(Software):*** يطلق أيضا على المكونات المعنوية للحاسوب بالبرمجيات، فهي بمثابة العمود الفقري وعصب عمل الحاسوب، إذ توفر إمكانات وسرعة فائقة في إنجاز المهام المطلوبة[4]. من جانب آخر، يُعرّف الكيان المنطقي للحاسوب لغة بأنه كلمة تستخدم للدلالة على جميع المكونات غير المادية لنظام الحاسوب كبرامج النظام الضرورية لتشغيله، إضافة إلى برامج التطبيقات التي تهدف إلى حل المشكلات المتعلقة باستعمال الحاسوب كما عرفه القانون الأمريكي الصادر سنة 1980 بأنه: "مجموعة توجيهات أو تعليمات يمكن للحاسب استخدامها بشكل مباشر أو غير مباشر للوصول إلى نتيجة معينة"[5]، وفي الاتجاه نفسه، عرف

---

[1] علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، بيروت، لبنان، ط1 2013، ص35.

[2] بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الإسكندرية مصر، 2008، ص22.

[3] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة للنشر الإسكندرية ، مصر 2009، ص ص 88-89 .

[4] بلال أمين زين الدين، المرجع السابق، ص23.

[5] طارق إبراهيم الدسوقي عطية، المرجع السابق، ص99.

التوجيه الأوروبي الصادر في: 14 ماي 1991 برامج الحاسب الآلي بأنها:" مجموعة من الأوامر التي تؤدي إلى إنجاز المهام المستهدفة من خلال نظام معالجة المعلومات والذي يطلق عليه إسم الحاسب"[1]. من جانب آخر يمكن تقسيم برامج الحاسوب إلى نوعين: الأول برامج النظام *(System Programs)*، والذي دونه لا يمكن تشغيل واستغلال الحاسوب، ويتضمن نظم التشغيل والبرامج المساعدة ونظام إدارة قواعد البيانات، والثاني برامج التطبيقات أو الكيانات المنطقية التطبيقية *(Application Programs)* ، والتي تقوم بمهام محددة مثل: برامج معالجة النصوص، أو برامج توجه لخدمة وظيفة معينة كبرامج إدارة الموارد البشرية...إلخ[2].

من جهة أخرى، تتميز المكونات المادية والمعنوية للحاسوب بخصائص عديدة، من بينها السرعة التي هي وثيقة الصلة بنوع ومقدرة برامج التشغيل، إضافة إلى الدقة في تنفيذ المهام ناهيك عن القدرة التخزينية الهائلة على نحو قد يتفوق على العقل البشري بما يوفر سهولة في أداء العمل وتمكين المستخدم من القدرة على التواصل بفضل وسائل الاتصال الحديثة كالإنترنت وغيرها، حيث مرّ الحاسوب بمراحل عديدة مثّلت تطوره التقني المذهل الذي وصل إليه اليوم.

ثانيا: التطور التاريخي للحاسوب: منذ منتصف القرن العشرين وحتى وقتنا الحاضر، شهدت الحواسيب سلسلة من التطورات في أجزائها المادية والبرمجية، والتي عرفت لاحقا بأجيال الحواسيب التي تتسم بخصائص فنية معينة كصغر الحجم والذاكرة الكبيرة والفعالية في الأداء، حيث تحول الحاسوب من نظام يعج بالشرائح والتوصيلات والدارات المتكاملة إلى مجرد رقاقة هي في حد ذاتها حاسبا، وعموما يمكن تصنيف الأجيال التي مّر بها الحاسوب إلى:

أ- **الجيل الأول:(1959-1951):** في بداية 1951 تم تطوير أول جهاز حاسب للأغراض التجارية يسمى: *(Univarcal)* استخدمت فيه تقنية الصمامات المفرغة التي تتميز بغلاء ثمنها وبطئها وتوليدها للحرارة العالية، كما كان حجم هذا الحاسب كبيرا ولغة برمجته صعبة ومعقدة مقارنة بلغات البرمجة التي ظهرت لاحقا[3].

---

[1] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، مصر، 2008، ص66.

[2] طارق إبراهيم الدسوقي عطية، المرجع السابق، ص100، راجع أيضا، بشرى النية، الحماية القانونية لبرامج الحاسوب، منشورات جمعية نشر المعلومة القانونية والقضائية-سلسلة الدراسات والأبحاث، الرباط، المملكة المغربية، العدد10، مارس2009، ص ص40-41.

[3] علي عبود جعفر، المرجع السابق، ص49.

ب- الجيل الثاني:(1959-1964): تميز هذا الجيل بظهور تقنية الترانزيستور *(Transistor)*[*] كاختراع جديد في عالم الإلكترونيات الذي يمتلك مزايا عديدة لا يمتلكها الصمّام المفرغ، حيث زادت سرعة تنفيذ العمليات الحسابية وانخفاض في الحجم والكلفة واستخدمت لغات برمجة جديدة مثل: لغة فورتران وكوبول[1].

ت- الجيل الثالث:(1964-1970): شهد هذا الجيل ولادة الدوائر المتكاملة *(Integrated Circuits)*، وهي عبارة عن مواد شبه موصلة نقية يتم إضافة شوائب إليها بطريقة دقيقة لتشكل ترانزستورات ومكثفات ومقاومات، حيث كان لها الأثر الكبير في تصغير حجم الحاسوب، وبالموازاة تم تحسين أجهزة الإدخال والإخراج بإضافة تحسينات على الأقراص المغناطيسية والشاشات[2].

ث- الجيل الرابع:(1970-1981): تميز هذا الجيل بتطوير تقنية الدارات المتكاملة مما زاد من سرعة العمليات، إضافة الى تطوير رقائق صغيرة جدا من مادة السيليكون *(Silicone)* تدعى: "المعالج الميكروي"، وفي هذا الجيل أيضا تم إدخال تحسينات هامة على أجهزة الإدخال والإخراج[3].

ج- الجيل الخامس:(1981-1991): أعلن اليابانيون عن مشروع الجيل الخامس للحاسبات الإلكترونية في مؤتمر عقد في طوكيو سنة 1981، وهذا نتيجة للتطور الفائق للذكاء الاصطناعي وإنتاج حاسبات تتميز بالقدرة على الاستنتاج وسرعة تصل إلى ألف(1000) مليون عملية في الثانية باستخدام وسائل المعالجة المختلفة[4].

ح- الجيل السادس:(1992 إلى وقتنا الحاضر): من خصائص هذا الجيل تقليد عمل الدماغ البشري والتشبه به، حيث تعتمد تقنيات هذا الجيل على عنصرين هامين: العنصر الأول يسمى بالشبكات العصبية التي تشمل تصميم برامج تحاكي الشبكة العصبية للدماغ، حيث يمكنها تفسير الكلام البشري وتشخيص الأجسام والصور بالأبعاد الثلاثة، والعنصر الثاني المعالجات المتوازية التي تمكن الحاسوب من القيام بحوالي 15 بليون عملية حسابية في الثانية، وهي بذلك تقارب سرعة الضوء[5].

---

[*] الترانزيستور *(Transistor):* عبارة عن قطعة معدنية صغيرة جدا على شكل حلقة ممغنطة تستعمل لتخزين المعلومات، مصنوع من لفافة سيليكون وهي مادة شبه موصلة مصنوعة من الرمل، وتتميز هذه المادة بأنها لا تدع التيار الكهربائي يمر عبرها بسهولة، كما أنها لا تمنعه من المرور، وبفضل هذه الاختراع صار الحاسوب أسرع وأقوى، نهلا عبد القادر المومني، المرجع السابق، ص31.

[1] المرجع نفسه، ص31.

[2] علي عبود جعفر، المرجع السابق، ص50.

[3] نهلا عبد القادر المومني، المرجع السابق، ص32.

[4] محمد حماد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2004 ، ص34.

[5] علي عبود جعفر، المرجع السابق، ص51.

الفرع الثاني : تعريف شبكة الإنترنت وتطورها التاريخي:

يشهد العلم تطورا مذهلا ومتسارعا في تكنولوجيا الاتصالات، حتى صارت وسائل الاتصال الحديثة وعلى رأسها شبكة الإنترنت أداة لا يمكن الاستغناء عنها، لذا سنتطرق أولا لتعريف الإنترنت، وثانيا إلى تطورها التاريخي.

أولا: تعريف شبكة الإنترنت: إن اصطلاح الإنترنت *(Internet)* هو اختصار لكلمتين إنجليزيتين: الأولى *(International)* والثانية *(Network)*، لها عدة تعاريف منها: "مجموعة شبكات وأجهزة الحاسب الإلكتروني التي تتواجد في مختلف دول العالم والتي تتصل ببعضها، ويجمع بينها أنظمة الاتصالات الإلكترونية التي تستخدم لنقل البيانات، أو ما يسمى: "بنظام نقل المعلومات" *(Transmission Control Protocol Internet)*، أو ما يعرف اختصارا بـ*(TCP/IP)*[1]، حيث تسمح الإنترنت بنقل كم هائل من النصوص والصور والصوت ومعطيات الأنظمة المعلوماتية مشكلة بذلك فضاء عالميا لتبادل المعلومات[2]. من جانب آخر تعتبر الإنترنت: "مجموعة من شبكات المعلومات الدولية التي ترتبط ببعضها، مما يتيح تبادل المعلومات بين البشر على اتساع العالم كله"[3]، كما تعرف أيضا على أنها: "شبكة عالمية دولية ووسيلة من وسائل الاتصال والتواصل بين الشبكات، تجمع مجموعة من شبكات الحاسب الآلي المرتبطة ببعضها البعض، إما عن طريق خطوط التليفون أو عن طريق الأقمار الاصطناعية وتعمل وفقا لبروتوكول*(TCP/IP)*، أو هي: "فن الاتصالات"[4]، حيث تقدم للإنسانية جملة من الخدمات كالبريد الإلكتروني وتبادل المعلومات...إلخ[5].

كما عرف أيضا القانون السعودي الصادر في: 2007/03/26 الشبكة المعلوماتية بأنها:" ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها مثل الشبكات

---

[1] *(TCP/IP)*: هما بروتوكولين معا وظيفتهما ضمان الاتصال بين عدة حواسيب عبر شبكة الإنترنت يعملان بشكل متزامن، أكثر تفاصيل راجع، عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة معمقة في جرائم الحاسب الآلي والإنترنت دار بهجات للطباعة والتجليد، القاهرة، مصر، 2009، ص ص63-64، وأيضا، خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، مصر، ط1، 2009 ، ص36.

[2] *Alain Bensoussan ,Internet aspects juridique, édition HERMES, Paris, France, 2e édition, 1998,p.197.*

[3] حسن طاهر داود، الحاسب وأمن المعلومات، مركز البحوث، الرياض، السعودية، 2000، ص339.

[4] *CHRISTIANE FERAL-SCHUHL, Le Droit à L'épreuve De L'INTERNET, DALLOZ, DUNOD, Paris, France, 2e édition, 2000,p.1.*

[5] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، دراسة متعمقة ومقارنة في جرائم الهاتف المحمول-شبكة الإنترنت والاتصالات-كسر شفرات القنوات الفضائية المدفوعة مقدما وذلك في قوانين فرنسا-مصر-الأردن-الإمارات-المغرب-عمان-قطر-البحرين-السعودية-فلسطين، المركز القومي للإصدارات القانونية، القاهرة، مصر، ط1، 2011، ص22 .

الخاصة والعامة والشبكة العالمية (الإنترنت)"[1]، كما أنها تعني لغويا :" الترابط الذي يتم بين الشبكات حيث أنها تتكون من عدد كبير من شبكات الحاسب الآلي المترابطة فيما بينها والمتناثرة في أنحاء كثيرة من العالم"[2]. أما اصطلاحا فتعني:" الوسيلة أو الأداة التواصلية بين الشبكات المعلوماتية دونما اعتبار للحدود الدولية"[3]، وعرّفها آخرون على أنها:" تلك الشبكة العنكبوتية التي تربط بين كم هائل من الحاسبات، مستعملة في عملية الربط هذه مختلف وسائل الاتصالات السلكية واللاسلكية، مثل: خطوط الهاتف أو الأقمار الصناعية أو كوابل الألياف البصرية *(Fiberoptic)*[4].

وبناء على هذا المفهوم لشبكة الإنترنت، يمكن لأي شخص يمتلك هاتفا نقالا ذكيا مزودا بتقنية الجيل الثالث*(G3)* أو الجيل الرابع *(G4)*، أو حاسوب مزود بجهاز مودم*(Modem)*، ومشترك في خدمة الإنترنت، الإبحار في هذا الفضاء السبراني*(Cyberspace)*[*] بكل حرية ودون قيود والاستفادة من الخدمات المتنوعة مثل: دخول المواقع المتنوعة وتحميل الملفات وإرسالها...إلخ.

بالنسبة للجزائر أدى الطلب المتزايد على استعمال شبكة الإنترنت، إلى قطع مراحل متقدمة في مجال توفير هذه الخدمة التي تمس كافة مجالات حياتنا، في هذا الصدد نشرت سلطة الضبط للبريد والمواصلات السّلكية واللاّسلكية على موقعها الرسمي تقريرا إحصائيا بعنوان سنة 2015[5] ، حيث بلغت مداخيل الهاتف الثابت والنقال 433 مليار دج، يرجع القسم الأكبر فيها إلى مشتركي تقنية الجيل الثالث*(3G)* بنسبة 92%، كما بلغت نسبة مشتركي الإنترنت 46% ويعود ذلك أساسا لإطلاق خدمة الجيل الثالث*(3G)* والرابع *(4G)*، وهذا ما يؤدي في حالة إساءة استخدام الحاسوب وشبكة الإنترنت والهاتف النقال إلى بروز جرائم مستحدثة، سُميت بالجرائم الإلكترونية أو الجرائم المعلوماتية كما سنرى لاحقا.

ثانيا: التطور التاريخي لشبكة الإنترنت: ظهرت فكرة النواة الأولى للإنترنت عندما أطلقت وزارة الدفاع الأمريكية مشروع شبكة وكالة الأبحاث المتقدمة *(ARPANET)* بهدف مساعدة الجيش الأمريكي لإيجاد أفضل طريقة للاتصال بعدد غير محدود من أجهزة الحواسيب لضمان استمرار

---

[1] خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص37.

[2] حسن بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت–دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2009 ص15.

[3] المرجع نفسه، ص15.

[4] طارق إبراهيم الدسوقي عطية، المرجع السابق، ص112.

[*] الفضاء السبراني: تعبير وصفه الروائي ويليام جيبسون ، ويقصد به :العوالم الافتراضية التي تخلقها الشبكات المعلوماتية، حسن بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص14.

[5] للاطلاع على تفاصيل هذا التقرير، راجع الموقع الرسمي لسلطة الضبط للبريد والمواصلات السلكية واللاسلكية الآتي: *http://www.arpt.dz/fr/#*، تاريخ الاطلاع:2016/05/02 على الساعة: 09:20.

الاتصالات في حال تعرض أمريكا لهجوم بسلاح نووي من قبل الاتحاد السوفياتي[1] أي: أن بداية ظهور شبكة الإنترنت كان لأغراض عسكرية بحتة، وفي سنة 1972 تطور المشروع وتحوّل إلى الاستعمال السلمي، نتيجة إسهامات طلبة وأساتذة الجامعات والمجتمع العلمي عموما، إلا أن الشبكة صارت تعاني ازدحام يفوق طاقتها وصار من الضروري إنشاء شبكة جديدة سميت: *(NSFNET)* بهدف السماح بدخول المجتمع العلمي كافة للمعلومات المخزنة، وكان ذلك سنة 1980.

ولقد انفصلت الشبكة العسكرية عن الشبكة الأم سنة 1983، والذي يعتبر تاريخ ميلاد شبكة الاتصالات الدولية، حيث سُمح لمختلف الأفراد باستعمالها وتم توصيل جميع شبكات الاتصال بمشروع شبكة وكالة الابحاث المتقدمة مستخدمين بروتوكولات الاتصالات نفسها ونظام التشغيل أو نظام *(UNIX)*. وفي سنة 1986 توسعت شبكة الإنترنت وشملت كثيرا من الجامعات والمعاهد ثم انتقلت إلى التطبيقات الكمبيوترية التجارية مكونة آلاف الشبكات، وقد نشأت الإنترنت من ترابط هذه الشبكات[2]. ثم ظهرت فكرة الـ*(WWW)* من المخبر الأوروبي لفيزياء الجسيمات والذي كان بحاجة لوسيلة تمكنه من متابعة الوثائق والمعلومات المتوفرة لديهم وتحديثها، وتم تطبيق هذا المشروع سنة 1992[3].

وتتميز شبكة الإنترنت بأنها شبكة حرّة بالرغم من عالميتها وعدم إلزامها بنطاق أو حدود معينة فهي مستقلة لا تخضع لسلطة دولة أو حكومة معينة أو تنظيم أو تيار، كما يمكن استخدامها في أي مكان وفي أي وقت، إذا توفرت الأدوات التقنية المناسبة لذلك، فهي تخلق عالما افتراضيا إلكترونيا يتبادل مستخدموها فيه كما هائلا من الاتصالات الصوتية والمصورة والمكتوبة والبيانات والمعلومات...إلخ، كما أنها تربط بين جميع مستخدميها في جميع أنحاء الكرة الأرضية[4].

المطلب الثاني: دور الحاسوب في مجال ارتكاب الجريمة

لا يجب الخلط بين دور الحاسوب في الجريمة الذي يكون إما الهدف المباشر للاعتداء مثل: حالة الدخول غير المصرح به للنظام المعلوماتي وهذا ما ستناوله في (الفرع الأول)، أو أداة ووسيلة لارتكاب الجريمة كاستغلال الحاسوب للاستيلاء على الأموال، والذي سنتطرق إليه في (الفرع الثاني).

[1] حنان ريحان المبارك المضحكي، الجرائم المعلوماتية –دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2014، ص13.

[2] خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص35.

[3] حنان ريحان المبارك المضحكي، المرجع السابق، ص ص15-16.

[4] المرجع نفسه، ص17.

الفرع الأول: الحاسوب هدفا للجريمة:

كما رأينا سلفا، يعتبر الحاسوب مجموعة من الأجهزة متكاملة مع بعضها البعض، بهدف تشغيل مجموعة من البيانات الداخلة وفقا لبرنامج موضوع مسبقا للحصول على النتائج المطلوبة، لذا قد يكون الحاسوب في حد ذاته محلا للجريمة، وهو المستهدف بمعنى: سرقة البيانات والمعلومات التي يختزنها الجهاز في ذاكرته، كما في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها أو الاستيلاء عليها لاستغلالها مثل[1]:

- سرقة المعلومات الخاصة بالتسويق لشركة أو مؤسسة، كسرقة قائمة بأسماء العملاء، وسرقة بيانات تتعلق بالإنتاج وأسعاره.
- الابتزاز مثل: سرقة بيانات تتعلق بالحياة الخاصة للأفراد.
- تخريب أو تدمير الممتلكات الذهنية بهدف عرقلة سير المؤسسة.
- سرقة براءات الاختراع المسجلة في الكمبيوتر وإنتاج نسخ مقلدة عنها لمصلحة الجاني.

إن من أوضح المظاهر لاعتبار الحاسوب هدفا للجريمة في حقل التصرفات غير القانونية عندما تكون السرية *(Confidentiality)* والتكاملية بمفهوم السلامة *(Integrity)*، هما الذين يتم الاعتداء عليهما، بمعنى أن توجه هذه الهجمات إلى معلومات الحاسوب أو خدماته، أو تعطيل قدرته وكفاءة أنظمته للقيام بأعمالها على أكمل وجه، وهدف هذا النمط الإجرامي هو نظام الحاسوب وبشكل خاص المعلومات المخزنة داخله، وغالبية هذه الأفعال الجرمية تتضمن ابتداء الدخول غير المصرح به إلى النظام، أو إدخال فيروسات للحاسوب، بحيث تعمل على تدمير البرامج المشغلة له أو إعاقتها أو نسخ كافة المعلومات المخزنة فيه[2].

في هذا الصدد يعرف الفيروس بأنه " برنامج حاسب مثل أي برنامج تطبيقي آخر، ولكن يتم تصميمه بواسطة أحد المجرمين لهدف محدد، وهو إحداث أكبر ضرر ممكن بنظام الحاسب، ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر ويتوالد ذاتيا، وهذا ما يتيح له قدرة كبيرة على الانتشار ببرامج الحاسب المختلفة، وكذلك بين مواقع مختلفة في الذاكرة، حتى يحقق أهدافه التدميرية"[3]. كما ينتشر أيضا عن طريق منافذ الدخول*(USB)* والأقراص الصلبة المتحركة أو عن طريق الاتصال بجهاز حاسوب مصاب بفيروس

---

1 حسين براهيم، الحاسب الآلي وتحديات القرن الحادي والعشرون، مجلة مركز بحوث الشرطة، أكاديمية الشرطة، مصر، العدد 14 1998، ص ص59-60.

2 يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت ، دار العدالة، القاهرة، مصر، ط1، 2011، ص24.

3 حسن طاهر داود، الحاسب وأمن المعلومات، المرجع السابق، ص71.

ما...إلخ[1]. للفيروسات أنواع كثيرة من أشهرها، فيروس ميليسا *(Melissa)* وفيروس حصان طروادة *(the Trojan Horse)*، وفيروس الحب*(Love Virus)*...إلخ.

ومع التطور السريع في أنماط ارتكاب الجرائم الإلكترونية، أصبح من الصعب وضع تصنيفات ثابتة للجناة، حيث يمكن تقسيم أنماط هؤلاء المجرمين إلى فئتين هما: الفئة الأولى تسمى: بالمخترقين أو القراصنة وهم معروفون باصطلاح: الهاكرز*(Hackers)*[2]، أما الفئة الثانية فيطلق عليها اسم: الكراكرز*(Crackers)*[3]. فمن خلال إحدى الدراسات التي أجراها معهد ستانفورد *(Stanford)* البريطاني، كشف أن 25%من أفعال الاعتداء على نظم المعالجة الآلية للمعطيات قام بها المحلّلون*(Analysts)*، و18 % قام بها المبرمجون*(programmers)*، و17% من الجرائم قام بها المستخدمون*(users)*، و16% قام بها الصرافون*(cashiers)*، و11 % قام بها المُشغّلون *(operators)*[4].

وقصد حماية الحاسوب من أن يكون هدفا للجريمة، ينصح خبراء المعلوماتية اتخاذ إجراءات بسيطة ولكنها فعّالة مثل: تفادي عملية تبادل الأقراص المضغوطة والأقراص الوميضية، وفتح رسائل البريد الإلكتروني مجهولة المصدر ...إلخ، إضافة إلى تنصيب برامج وتطبيقات غير معروفة المنبع كما تبرز أيضا ضرورة تنصيب برامج حماية للحاسوب *(Antivirus)* يتم تحديثها دوريا لمنع دخول الفيروسات وصد أي اختراق محتمل.

---

[1] *Myriam Quéméner et Joel Ferry, Cybercriminalité Défi mondial, Economica, France, 2e édition 2009, pp. 75-78.*

[2] هاكرز*(Hackers)*: تعود أصل كلمة هاكرز إلى ستينيات القرن العشرين، حيث وُصف مبرمجو تلك الفترة بالهاكرز نظرا للخبرة الواسعة والتعامل السلس مع أسطر الأوامر، وحل جميع المشاكل البرمجية وتمكنهم من برمجة لوغاريتمات تفهمها الحواسيب، فهم متطفلون من فئة مراهقين وشباب يتحدون إجراءات أمن النظم والشبكات، لكن لا تتوافر لديهم في الغالب دوافع تخريبية أو حاقدة، وإنما ينطلقون من دوافع شخصية لإثبات ذواتهم، ومنه فالهاكر هو: أي شخص قادر على التعامل مع الكمبيوترات والأجهزة الرقمية بخبرة ودراية، وكذا قادرا على إنشاء وحل مشاكل داخل هذه الأنظمة، حتى ارتبطت كلمة هاكر مع الشر فأصبح الشائع لدى العامة أنه ذلك الشخص السيئ الذي يسرق معلوماتهم الهامة ويخرّب أجهزتهم ويتسبب لهم في خسائر مادية ومعنوية رغم أنهم لم يفعلوا له شيء. مصطفى محمد موسى أساليب إجرامية بالتقنية الرقمية، ماهيتها، مكافحتها، -دراسة مقارنة، دار الكتب القانونية، مصر، 2005، ص 15، راجع أيضا *Mohammed Buzubar, La Crime Informatique Sur L'internet, Journal Of Law, ,Annéé26eme, University of Kuwait, N° :1,mars 2002,p.44.*، وأيضا، حسن مظفر الرزو، الأمن المعلوماتي (معالجة قانونية أولية)، مجلة الأمن والقانون أكاديمية شرطة دبي، الإمارات العربية المتحدة، العدد 1، السنة الثانية عشر، جانفي 2004، ص79.

[3] الكراكرز*(Crackers)*: أشخاص يتميزون بسعة الخبرة والإدراك الواسع للمهارات التقنية، يقومون بالتسلل إلى نظم المعالجة الآلية للمعطيات قصد الاطلاع على البيانات المخزنة فيها لسرقتها أو العبث بها، تتراوح أعمارهم بين 25 و45 سنة، أو هو:" كل شخص يمارس عملية تصديع كلمات العبور المصاحبة للنظم المعلوماتية، أو يباشر عملية فك الشيفرات الخاصة بحماية النظم البرمجية التطبيقية بشتى أنواعها، راجع، حسن مظفر الرزو، المقال السابق، ص87، راجع أيضا، *Mohammed Buzubar,art-Cit,p.47*

[4] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص43.

الفرع الثاني: الحاسوب أداة لارتكاب للجريمة:

بعد أن أوضحنا أن الحاسوب يمكن أن يكون هدفا للجريمة، لكنه يمكن أن يكون أيضا أداة أو وسيلة لارتكاب الجرائم الإلكترونية المتنوعة، ويتم ذلك بأن يتقدم المجرم ببرنامج *(software)* يستطيع بموجبه أن يتحاور مع الحاسوب *(to manupulate)*، بمعنى يتحاور مع البرامج أو النظم المبرمجة في الحاسوب ويحولها إلى عمل غير مشروع، كما في حالة استغلال الحاسوب للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف والتزوير أو استخدام التقنية في الاستيلاء على أرقام بطاقات الائتمان وإعادة استخدامها للحصول على الأموال[1].

من جانب آخر قد يستخدم الحاسوب في جرائم القتل، كما في الدخول إلى قواعد البيانات الصحية والعلاجية وتحويرها، أو تحوير عمل الأجهزة الطبية والمجهرية عبر التلاعب ببرمجياتها أو قرصنة برمجيات التحكم في الطائرة أو السفينة بشكل يؤدي إلى تدميرها وقتل ركابها[2]. وهذا ما عالجه المشرع الجزائري بموجب القانون رقم: 04-15 مؤرخ في 2004/11/10 يعدل ويتمم قانون العقوبات بإضافة قسم سابع مكرر عنوانه: "المساس بأنظمة المعالجة الآلية للمعطيات[3]، حيث كان الهدف هو حماية نظام المعالجة الآلية للمعطيات من الجرائم الإلكترونية كما سنرى لاحقا.

كما يمكن للحاسوب أيضا أن يكون بيئة مناسبة لارتكاب الجرائم الإلكترونية، ومثال ذلك: تخزين البرامج المقرصنة فيه، أو في حالة استخدامه لنشر المواد غير القانونية أو استخدامه أداة تخزين أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية وشبكات الاتجار بالبشر...إلخ. من جهة أخرى، للحاسب دور مهم في اكتشاف الجريمة، إذ يستخدم على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم، ناهيك عن اعتماد الجهات القضائية المختصة بالتحقيق في الجرائم الإلكترونية على أحدث النظم والبرامج المعلوماتية في إدارة مهامها، وذلك من خلال بناء قواعد البيانات *(databases)* المتضمنة لمعلومات دقيقة حول المجرمين، أو من خلال استعمال برامج متطورة للتعرف على الوجوه والبصمات...إلخ. ومع تنوع واتساع نطاق جرائم الحاسوب، واعتماد مرتكبيها على أساليب ووسائل متطورة توفرها تقنية المعلومات، صار لزاما على الأجهزة القضائية استخدام الوسائل نفسها للكشف عنها، يعني ذلك أنه بقدر استغلال المجرم المعلوماتي التقنية المتطورة في مجال استعمال الكمبيوتر والإنترنت، بقدر استعمالها أيضا في مجال الكشف عنه وملاحقته

---

[1] حسين براهيم، المقال السابق، ص91.

[2] يوسف أبو الحجاج، أشهر جرائم الكمبيوتر والإنترنت ، دار الكتاب العربي، دمشق، سوريا، ط1، 2010، ص34.

[3] القانون رقم: 04-15 المؤرخ في: 2004/11/10 يعدل ويتمم الأمر رقم: 66-156 المؤرخ في: 8 يونيو 1966 والمتضمن قانون العقوبات، (ج. ر) رقم:71 المؤرخة في:2004/11/10، ص ص8-11.

وضمان عدم إفلاته من العقاب، مع ملاحظة أن هذه المهمة تتطلب الاهتمام بالتكوين النظري والتدريب العملي المتواصل للمكلفين من السلطة القضائية المختصة بالتحقيق في الجرائم الإلكترونية قصد اكتساب المهارات التقنية اللازمة للتعامل مع هذا النوع المستحث من الجرائم.

المطلب الثالث: دوافع ارتكاب الجرائم الإلكترونية

حتى يتمكن المشرع الجنائي من وضع سياسة جنائية فعّالة في مجال مكافحة الجرائم الإلكترونية، لا بد له من تصور واضح وكامل حول الدوافع الشخصية للمجرم المعلوماتي لارتكاب جرائمه(الفرع الأول)، وأيضا دون إهمال للدوافع الخارجية التي تلعب دورا هاما، والتي سنتعرف على بعض منها في (الفرع الثاني).

الفرع الأول: الدوافع الشخصية:

لا يخفى على أحد أن المجرم يرتكب جريمته نتيجة دوافع معينة، تختلف هذه الدوافع من مجرم لآخر كما قد تكون مشتركة بينهم، والأمر نفسه بالنسبة للمجرم الإلكتروني الذي يرتكب جريمته في بيئة إلكترونية تختلف تماما عما نعرفه عن البيئة التقليدية. إذ يمتلك دوافع شخصية عديدة، وعموما يمكن تقسيمها إلى دافعين رئيسين هما:

أولا: الدوافع المالية: وفيها يكون الهدف من ارتكاب الجرائم الإلكترونية على اختلاف أنواعها هو الحصول على ربح مالي عن طريق المساومة على البرامج أو المعلومات المتحصلة بطريق الغش من الحاسوب أو باستعمال بطاقة سحب آلي منتهية الصلاحية[1]، ففي إحدى الدراسات التي أجرتها مجلة متخصصة في الأمن المعلوماتي تبين أن 34% من الجرائم كان هدفها اختلاس الأموال، نتيجة ما يعانيه المجرم مثلا من تراكم للديون الناجمة عن المشكلات العائلية أو الخسائر الناجمة عن لعب القمار أو إدمان المخدرات...إلخ[2]. فيقوم هؤلاء المجرمون باستغلال قدراتهم وكفاءاتهم الفنية في مجال تقنية الحواسيب وشبكات الإنترنت للسطو على البنوك والتلاعب في أنظمتها وسرقة أموال منها وتحويلها، أو بيع المعلومات المختلسة الذي يعتبر مجالا لنشاط إجرامي متسع للغاية[3].

ثانيا: الدوافع الذهنية أو النمطية: قد لا يكون المال دائما هو الدافع وراء ارتكاب الجرائم الإلكترونية، بل قد تكون الرغبة في إثبات الذات، وقهر النظام الحاسوبي وتخطي حواجز الحماية وإثبات التفوق العلمي وإظهار القدرات والمهارات في مجال تقنيات الحاسوب. والملاحظ هنا أن فئة

---

[1] محمد أمين الرومي، المرجع السابق، ص24.

[2] أحمد خليفة الملط، الجرائم المعلوماتية–دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، ط2، 2006، ص89.

[3] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، مصر، ط1، 1994 ، ص50.

هؤلاء المجرمين هم من صغار السن ونوابغ المعلوماتية يحاولون إثبات تفوقهم العلمي والعملي في مجال المعلوماتية وشبكة الإنترنت[1].

الفرع الثاني: الدوافع الخارجية:

تتعدد هذه الدوافع ويمكن تقسيمها إلى ما يأتي:

أولا: دافع الانتقام: وذلك حينما تتوفر لدى المجرم الرغبة في الانتقام، فقد دفع الانتقام بمحاسب شاب إلى التلاعب بالبرامج المعلوماتية، بحيث بعد مضي أشهر من مغادرته للمؤسسة التي كان يعمل بها، يتم تدمير كل البيانات والحسابات الخاصة بديون هذه المؤسسة، وقد تحقق ذلك فعلا والأمثلة كثيرة في واقعنا فحينما يلجأ أصحاب المؤسسات الخاصة إلى الاستغناء عن خدمات بعض مهندسيها في المعلوماتية أو طردهم تعسفيا، قد يلجأ هؤلاء بدافع الانتقام إلى استعمال مهاراتهم في ارتكاب جرائم إلكترونية مثل: جريمة الدخول غير المشروع للحاسوب بقصد نسخ أو تدمير معطيات أو الاعتداء على نظام المعالجة الآلية للمعطيات...إلخ، وذلك لإلحاق أكبر ضرر بالمؤسسة[2].

ثانيا: دافع جنون العظمة أو الطبيعة التنافسية: ويكون ذلك من خلال الموظفين داخل المؤسسة بغية إظهار ملكاتهم الفنية في هذا المجال لخلق جو من المنافسة قصد الوصول للمراكز المرموقة داخل المؤسسة[3].

ثالثا: دافع التعاون والتواطؤ على الأضرار: يحدث هذا كثيرا في الجرائم المعلوماتية، حيث يقوم متخصص في الأنظمة المعلوماتية يعمل لدى المؤسسة بالتعاون مع شخص آخر من محيط أو خارج المؤسسة بتغطية عمليات التلاعب وتمويل المكاسب المادية، عن طريق اختراق الأنظمة المعلوماتية وتبادل المعلومات فيما بينهما[4] .

رابعا: دوافع خاصة بالمؤسسة: يظهر هذا الدافع من داخل المؤسسة نفسها، وذلك حينما يضع مدير المؤسسة ثقته في الشخص المسؤول عن الأنظمة المعلوماتية، غير أن هذا الأخير يستغل منصبه في قضاء مصلحته الشخصية عن طريق توظيف مهاراته الفنية في استخدام تقنيات الحاسوب للحصول على مكاسب مادية، وبالتالي يصل الأمر لحد ارتكاب جرائم معلوماتية خطيرة تضر بمصالح المؤسسة، ومثال ذلك "الاستخدام غير المشروع للنظام المعلوماتي من طرف مستشار لدى

---

[1] سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية مصر ،2010، ص93.

[2] الرسالة نفسها، ص94.

[3] أحمد خليفة الملط، المرجع السابق، ص90.

[4] المرجع نفسه، ص90.

إحدى البنوك الكبرى يدعى ستانلي ريفكن *(Stanley Rifkin)* كان يتمتع بثقة مطلقة من جانب البنك، حيث سمحت له اختصاصاته بالولوج لمفتاحين إلكترونيين من ثلاثة أساسية للتحكم في التحويلات الإلكترونية للنقود من بنك لآخر، وقد تمكن بفضل تألفه الشديد مع النظام المعلوماتي من الوصول إلى المفتاح الثالث أين استطاع تحويل 10 مليون دولار إلى حساب بنكي مفتوح باسمه في سويسرا، وألقي القبض عليه وصدر حكم ضده بالسجن لمدة ست سنوات[1].

وعليه تتعدد دوافع المجرم المعلوماتي في ارتكاب جرائمه سواء كانت شخصية أو متعلقة بالمؤسسة، وهذا ما ترجمه المشرع الجزائري في سياسته الجنائية المتعلقة بمكافحة الجرائم المعلوماتية في شق التجريم بتعديل قانون العقوبات بإضافة قسم سابع مكرر تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات" من المادة (394مكرر-394 مكرر7)، أين نص على جملة من الجرائم يقوم بها المجرم تنفيذا لدوافعه العديدة التي ينتج عنها أضرار بالغة، كجريمة الدخول أو البقاء عن طريق الغش في منظومة معلوماتية، أو جريمة حذف أو تغيير لمعطيات منظومة، أو جريمة تصميم أو بحث أو نشر أو الاتجار في المعطيات المخزنة...إلخ، وهذا ما سنتطرق إليه لاحقا بالتفصيل.

المطلب الربع: أضرار الجرائم الإلكترونية

أدى سوء استعمال تكنولوجيات الإعلام والاتصال إلى بروز جرائم مستحدثة، لم تكن معروفة من قبل، تتسبب في أضرار اقتصادية ومالية بالغة (الفرع الأول)، ليس هذا فقط، وإنما تعدى ذلك إلى وقوع أضرار على المستوى النفسي والاجتماعي، وهذا ما سنراه في (الفرع الثاني).

الفرع الأول: الأضرار الاقتصادية:

تتزايد أضرار الجرائم الإلكترونية يوما بعد يوم تبعا للتقدم المذهل في مجال تقنية المعلوماتية واستغلالها في المعاملات الاقتصادية والمالية الوطنية والدولية، ناهيك عن الاعتماد عليها في تسيير شؤون الحياة اليومية سواء بالنسبة للأفراد أو الحكومات، مما ينتج عنه أضرارا بالغة وخسائر كبيرة ففي دراسة أعدتها شركة ماكافي*(McAfee)* -وهي شركة رائدة في مجال إنتاج برامج مضادة للفيروسات- وقدمت لمؤتمر دافوس الاقتصادي، بلغت خسائر الجرائم الإلكترونية سنة 2008 فقط حوالي 1000مليار دولار، وهي تتجاوز بذلك مداخيل تجارة المخدرات[2]، وهو رقم ضخم جدا. كما نشر مكتب التحقيقات الفدرالي*(FBI)* استبيانا بتاريخ: 2001/04/12 شارك فيه أكثر من 500 مسؤول عن أمن المعلومات، أعلن فيه أن الجرائم الإلكترونية في تزايد مستمر حيث زادت ثلاثة

---

[1] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2007، ص58.

[2] *Ali EL AZZOUZI, La Cybercriminalité au Maroc, Bishoop solution, Casablanca, Maroc, 1ere édition,2010,p.18.*

أضعاف عن نهاية العام الماضي، كما بين هذا الاستبيان أن نسبة 85 % من المستطلع آراءهم تعرضت مؤسساتهم لجرائم معلوماتية تسببت في خسائر لـ 36 %منهم قدرت بـ378 مليون دولار [1].

من جانب آخر تقدر الأرباح العائدة من وراء بيع برامج الفيروسات حوالي 275 مليون دولار سنويا، ناهيك عن سرقة معلومات بطاقات الائتمان البنكية والبريد الإلكتروني...إلخ[2]. وفي تقرير آخر نشرته المجموعة الاقتصادية الأوروبية حول خسائر الجرائم المرتكبة بواسطة النظام المعلوماتي (الغش، الاحتيال، السرقة، التخريب...إلخ) بلغت حوالي 64.50 مليون أورو، كما أظهرت دراسة أيضا في المملكة المتحدة أن معدل خسارة كل حالة من حالات الاحتيال باستخدام النظام المعلوماتي بلغ 31000.00 جنيه استرليني، وهذا الرقم في تزايد مستمر [3].أما في فرنسا فقد ارتفع حجم الخسائر الناشئة عن أفعال التحايل المعلوماتي، حيث قدر المبلغ بحوالي 1.700.000.00 أورو، متعلقة أساسا بجرائم سرقة البرامج، كبرامج التصميم وإدارة البيانات والأمن وصيانته، وإفشاء الأسرار المعلوماتية...إلخ[4]، كما تسبب فيروسات الكمبيوتر أضرارا كبيرة مثل ما حدث سنة 2000 عندما تمكنت مجموعة من الشباب من نشر فيروس(الحب) على أجهزة الكمبيوتر الخاصة ببنك يونيون وبنك أوف سويتزرلاند، ومصرفين آخرين في الولايات المتحدة الأمريكية بهدف الوصول للأرقام الخاصة بمواقعها على شبكة الإنترنت [5].

من جانبها كشفت شركة *(Kaspersky)* الرائدة في مجال الأمن المعلوماتي، عن تفاصيل اختراق وسيطرة مجموعة من الهاكرز لحسابات في بنوك عالمية، وسرقة نحو مليار دولار حيث نجحوا في استخدام تقنيات معقدة من أجل الوصول لحسابات في بنوك عالمية، حيث لاحظ مواطنون في العاصمة الأوكرانية كييف سنة 2013 أن صرّافا آليا *(ATM)* تعطل وبدأ في إلقاء النقود بشكل عشوائي من دون إدخال أي بطاقة بنكية، كما ذكرت الشركة أن الهاكرز لم يستغلوا نقاط الضعف في برامج حماية بيانات الحسابات، لكنهم بدلا من ذلك قاموا باستغلال ثغرة بأنظمة أجهزة الحاسوب في البنوك، تمكنوا خلالها من نسخ بيانات الحسابات في مدة لا تتجاوز 20 ثانية واستغلوها من أجل تحويل الأموال بسرعة فائقة. أما بالنسبة للشركات فتتمثل في سرقة دعامات تخزين المعطيات والدخول عن طريق الغش لأنظمتها المعلوماتية للحصول على البيانات واعتراض المراسلات وشراء

---

[1] أحمد خليفة الملط، المرجع السابق، ص96.

[2] *Myriam Quéméner et Joel Ferry, Op.Cit,p.72.*

[3] أحمد خليفة الملط، المرجع السابق، ص99.

[4] بلال أمين زين الدين، المرجع السابق، ص ص37-38.

[5] عماد مجدي عبد الملك، المرجع السابق، ص29.

ولاء الموظفين للمساعدة في ارتكاب هذه الجرائم، مما كبّد هذه الشركات منذ سنة 2000 حوالي 1600 مليار دولار وتضييع 3.3% من أوقاتها في ترميم أنظمتها المعلوماتية المخربة[1].

من خلال ما سبق ذكره، تضر الجرائم الإلكترونية بصورة كبيرة بالمصالح الاقتصادية للدول خاصة في ظل التوجه الحديث نحو الاعتماد أكثر على التجارة الإلكترونية التي تتم في هذه البيئة الافتراضية، مما يصعب من عمل الجهات القضائية المختصة في البحث والتحري لكشف الجناة.

لكن في المقابل، هل اقتصر الأمر على الأضرار الاقتصادية فقط، أم تعدى ذلك إلى نوع آخر من الأضرار؟.

الفرع الثاني: الأضرار النفسية والاجتماعية:

توفر التقنيات الحديثة في مجال الحوسبة والاتصال خدمات جليلة في شتى الميادين لا يمكن للإنسان المعاصر الاستغناء عنها، لكن بالمقابل أدى سوء استعمالها إلى بروز جرائم مستحدثة لم تمس بالكيان الاقتصادي والمالي فحسب، ولكن مست أيضا بالكيان النفسي والاجتماعي لكافة فئات المجتمع، سواء كانوا أشخاصا بالغين أو أطفالا مراهقين، مما يجعلهم عرضة لهذه الجرائم التي تقودهم مبكرا لسلوك عالم الانحراف كجرائم الإباحية والاستغلال والتحرش الجنسي والاحتيال، لذلك يحتاج الأطفال والمراهقون إلى المراقبة المستمرة من طرف الوالدين قصد حمايتهم من سلبيات هذا العالم الافتراضي. كما يمكن أن تكون هذه التقنية وسيلة للتجسس على الأسرة بما يهدد كيانها ويؤدي إلى تفككها وبالتالي التأثير سلبا على وحدة وتماسك المجتمع، ومثال ذلك: كثرة حالات الطلاق والخيانة الزوجية بسبب انتشار غرف الدردشة الإلكترونية التي تعتبر فضاء حرا للاتصال بين الأشخاص وإبداء الرأي ونقل الانشغالات وتبادل الأفكار والمعلومات فيما بينهم بالصوت والصورة...إلخ[2].

وتجدر الإشارة هنا إلى ما وقع في الجزائر في سنة2016 من تسريبات لامتحانات شهادة البكالوريا، وذلك بنشرها عبر موقع التواصل الاجتماعي*(Facebook)* لتسهيل عملية الغش، أين تسببت هذه العملية في أضرار نفسية بالغة على المترشحين نتيجة إعادتهم الجزئية لها، إضافة إلى أضرار اقتصادية تمثلت في تكاليف إعادة وتأطير هذه الامتحانات.

ومنه يمكن القول: أن ظاهرة الإجرام المعلوماتي تؤثر سلبا على الطبقات الاجتماعية كافة فتزيد الهوة بينها بمقدار ما تملك من معلومات فيجد أصحاب الجريمة المنظمة الفضاء الإلكتروني مناخا مناسبا لهم، وتجد العصابات الإرهابية شبكة الإنترنت خير وسيلة لنشر أفكارهم، كما يتعدى

---

[1] *Myriam Quéméner et Yves Charpenel, Cybercriminalité Droit pénal appliqué, Economica, France, pp.9-11.*

[2] *CHRISTIANE FERAL-SCHUHL, Le Droit à L'épreuve De L'INTERNET, DALLOZ, France, Quatrième édition, 2006,p.573.*

ذلك إلى المستوى السياسي، حيث يجد العابثون والمعارضون لأنظمة الحكم في شبكة الإنترنت ضالتهم في ممارسة أساليب الضغط السياسي واستغلال هذه التقنية في الترويج للأفكار التي تتناسب مع مصالحهم، وذلك باستعمال المواقع الإلكترونية، وفضاءات التواصل الاجتماعي مثل: الفايسبوك *(Facebook)* وتويتر*(Twitter)*، *والأنستغرام (Instagram)*...إلخ[1].

وبناء على ما سبق، هناك العديد من الأضرار النفسية والاجتماعية التي تسببها تكنولوجيا المعلومات إن لم يحسن استخدامها وخصوصاً لدى فئة الأطفال والمراهقين، ويمكن إجمالها في النقاط الآتية[2]:

أولا: اكتشاف مواد غير ملائمة: فأحد المخاطر تتمثل باكتشاف الطفل لمواد غير ملائمة لسنه كمواد جنسية أو مواد تحث على الكراهية أو العنف أو تشجع الطفل أو المراهق على القيام بأعمال خطيرة أو غير قانونية أو تدعوه للتمرّد على الأسرة .

ثانيا: التحرش الجسدي: عندما يكون الطفل أو المراهق مرتبطا مباشرة بالإنترنت *(online)* فإنه قد يقوم بتوفير معلومات أو تهيئة لقاء غير متوقع قد يعرضه أو يعرض أحد أفراد عائلته إلى الخطر مثل: تظاهر بعض الشواذ المتعلقين بالأطفال بأنهم أصدقاء لأسرهم باستخدام البريد الإلكتروني أو لوحة إعلانات الإنترنت أو غرف الدردشة *(chat)* لكسب ثقة الأطفال واستدراجهم إلى لقاءات دون معرفة أسرته، ومن ثمة الاعتداء عليهم.

ثالثا: المضايقات: كاستلام رسائل بريد إلكتروني أو رسائل دردشة أو رسائل لوحة إعلانات الإنترنت تحمل مضايقات أو احتقارا أو روحا عدائية .

رابعا: سوء استخدام بطاقات الائتمان والتعدي على حقوق الغير: قد يقوم الطفل أو المراهق باستخدام بطاقات الائتمان الخاصة بوالديه أو أحد أفراد أسرته عبر الشبكة، أو بالتعدي على الحقوق الفردية للغير دون إدراكه للمسؤولية القانونية المترتبة على عمله، كما يؤدي هذا الفعل لدى البالغين إلى حدوث جرائم السرقة باستعمال بطاقات الائتمان وجرائم الاحتيال والتزوير...إلخ.

خامسا: خطر مجموعات الدردشة: توفر التقنية المعلوماتية وشبكة الإنترنت سهولة التواصل بين الأفراد أينما كانوا، ودونما اعتبار للحدود الجغرافية حتى صار العالم عبارة عن قرية صغيرة فيمكن استعمال تقنية غرف الدردشة للتواصل مع الآخرين، وهذا يشكل خطرا كبيرا خاصة على فئة

---

[1] *Redouane Semlali, Cybercriminalité :menaces et contre-mesures , Digital Maghreb, Maroc, N :4, fevrier-mars2013, pp.42-43.*

[2] منصور بن عبد الرحمن بن عسكر، دور المؤسسات الاجتماعية في التبصير من جرائم تقنية المعلومات، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 06، الثلاثي الأول، 2012، ص12.

المراهقين والأطفال، فقد يقومون بالدخول إلى مجموعات دردشة ويشتركون في نقاشات قد تسبب في تغيير معتقداتهم واعتناق أفكار هدامة دخيلة على مجتمعاتهم، مما يتسبب في عدم تجانس النسيج الاجتماعي للمجتمع.

سادسا: استلام رسائل البريد الإلكتروني مجهولة المصدر: وهي عادة تحوى إعلانات عن مواقع إباحية أو مواقع تجارة إلكترونية غير مشروعة، أو مواقع قمار أو مواقع لتجارة الجنس وغير ذلك، وبالتالي تساهم في انتشار جرائم متنوعة، كالجرائم الأخلاقية التي تؤدي إلى إفساد المجتمع[1].

ورغم إيجابيات تكنولوجيات الإعلام والاتصال في التقريب بين الشعوب والحضارات، إلا أنها أدت أيضا إلى تقليص العلاقات الاجتماعية مثل: ظهور مدمني الإنترنت الذين يبقون لوحدهم لساعات طويلة أمام الحاسوب، مما يتسبب في فتور العلاقة وبث الشكوك بين أفراد الأسرة الواحدة وقد يؤدي ذلك إلى تفككها، كما ينتج عنه صعوبة في التكيف مع الآخرين وعدم فتح مجالات للحوار والاندماج مع المجتمع والأسرة، وضمان بقاء السلوك الأسري داخل الإطار الذي يجب أن يكون عليه بلا مغالاة أو تعقيدات أو تجاوزات لقيم الأسرة، مما يضمن لنا الابتعاد على انتشار المزيد من التفكك الأسري وارتفاع نسبة الطلاق ومعدلات الانحرافات الأخلاقية والعنف، ولذلك لابد من التوعية المستمرة لخطورة الاستخدام السيئ لتقنية الحاسوب والإنترنت لآثارها السلبية على الفرد والمجتمع.

وأخيرا ومن خلال دراسة الأضرار الاقتصادية والنفسية والاجتماعية للجرائم الإلكترونية، يمكننا تحديد بعض أهداف مرتكبي الإجرام الإلكتروني وذلك كالآتي:

1- الوصول إلى المعلومات بشكل غير شرعي، كسرقة المعلومات أو الاطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم.

2- الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها.

3- الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم.

4- الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل: عمليات اختراق وهدم وتعطيل المواقع على شبكة الإنترنت وتزوير بطاقات الائتمان وسرقة الحسابات المصرفية وغيرها.

فبعد التطرق إلى تعريف الحاسوب وشبكة الإنترنت وتطورهما التاريخي، ودور الحاسوب في مجال ارتكاب الجرائم الإلكترونية، إضافة الى دوافع المجرم المعلوماتي لارتكاب جرائمه، لنخلص في

---

[1] المقال نفسه، ص13.

الأخير إلى مختلف الأضرار الناجمة عنها، ننتقل في المبحث الثاني للحديث عن كل ما يتعلق بمفهوم الجريمة الإلكترونية.

المبحث الثاني: مفهوم الجريمة الإلكترونية

نظرا للطبيعة الخاصة للجرائم الإلكترونية، اختلف الفقه في وضع تعريف مانع وجامع لها فأحيانا يكون الحاسوب وسيلة لارتكابها بواسطة الإنترنت وأحيانا أخرى يكون هدفا لها. سنتناول في هذا المبحث تعريف الجريمة الإلكترونية (في المطلب الأول)، ثم نتطرق إلى تصنيف الجريمة الإلكترونية وأنواع المجنى عليهم في (المطلب الثاني)، بعد ذلك نحاول تحديد الطبيعة القانونية للجريمة الإلكترونية في (المطلب الثالث)، وأخيرا نتناول خصائص الجريمة الإلكترونية ومراحل ارتكابها إضافة إلى مميزات المجرم الإلكتروني في(المطلب الرابع).

المطلب الأول: تعريف الجرائم الإلكترونية

تعتبر الجرائم الإلكترونية من الظواهر الحديثة نظرا لارتباطها بتقنية متطورة هي تكنولوجيا المعلومات والاتصالات مما صعّب من وضع تعريف جامع لها، لذا بذل الفقهاء جهودا مضنية في محاولتهم وضع تعريف لها ، حيث برز اتجاهان هما: الاتجاه الأول يعرف بالاتجاه الضيق في تعريفه للجرائم الإلكترونية، ويعرف الثاني بالاتجاه الموسع لها(الفرع الاول) ، لنخلص في الأخير إلى توضيح موقف المشرع الجزائري من هذه المسألة في(الفرع الثاني).

الفرع الأول: تعريف الفقه للجريمة الإلكترونية:

مما يلاحظ في هذا الشأن هو عدم وجود اتفاق سواء على المستوى التشريعي أو الفقهي على استعمال مصطلح معين للدلالة على هذا الظاهرة الجرمية الناشئة في بيئة الكمبيوتر والإنترنت، وهو اختلاف رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات والاتصالات، فهناك من يطلق عليها مصطلح جرائم الغش المعلوماتي، أو الجرائم المعلوماتية، أو الجرائم الإلكترونية، أو جرائم الحاسب الآلي، أو جرائم تقنية المعلومات، أو الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أو جرائم التكنولوجيا الحديثة، أو جرائم الكومبيوتر والإنترنت، ويرجع السبب في ذلك إلى عدة عوامل منها التطور المستمر واللاّمتناهي لتكنولوجيا المعلومات والاتصالات، مما نتج عنه جرائم مستحدثة اختلفت التشريعات حول وضع مفاهيم موحدة لها[1]. وقد يكون السبب أيضا ترك المجال أمام المشرع لاحتواء التقنيات المتلاحقة في هذا الميدان، ولعدم حصر قاعدة التجريم في نطاق أفعال معينة تتبدل في المستقبل. ويثير هذا الإشكال العديد من التحديات أهمها صعوبة مواجهتها وتعذر الحلول المناسبة

---

[1] *Nidal El Chaer, La Criminalité Informatique Devant La Justice Pénale, édition juridique sader,Beyrouth,Liban,2004,pp.18-19.*

لمكافحتها سواء على المستوى الداخلي أو الدولي[1]. ورغم هذه الصعوبات حاول الفقهاء جاهدين وضع مفهوم لهذه الجرائم المستحدثة أين برز اتجاهان هما:

أولا: الاتجاه الضيق لمفهوم الجرائم الإلكترونية: حاول هذا الاتجاه حصر مفهوم الجريمة الإلكترونية وربطها بعناصر عديدة كالحاسوب، أو مستخدمه، أو بموضوع الجريمة، حيث عرفها الفقيه ماروي *(Merwe)* على أنها:" الفعل غير المشروع الذي يستخدم في ارتكابه الحاسب الآلي"[2] وهناك من عرفها على أنها:" فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه"[3]، أو هي: "الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الانترنيت"[4]. كما عُرفت أيضا بأنها: " الجرائم التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط"[5]، أو هي: "مجموعة المخالفات الجزائية التي تقع ضد شبكات الإعلام الآلي"[6] وفي تعريف آخر هي:" الأفعال غير القانونية المرتكبة بواسطة العمليات الإلكترونية والتي تمس بالنظام المعلوماتي أو بالمعطيات التي يحتويها ومهما كان الهدف من ذلك[7]. من جانب آخر عرفها الفقيه روزبلات *(Rosblat)*:"كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومة المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه"[8]، كما عرفها الفقيه الألماني تادمان *(Tiedemann)* على أنها:" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب"[9]. من جهة أخرى، عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها:" الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[10].

وعليه يربط أنصار هذا الاتجاه تعريفهم لهذه الجرائم بضرورة وجود الحاسوب الذي قد يكون أداة للجريمة أو هدفا لها، ناهيك عن وجود معارف مسبقة بتكنولوجيا الكمبيوتر ليس فقط من المجرم

---

[1] خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص73.

[2] عبد العال الديربي ومحمد صادق إسماعيل، المرجع السابق، ص40.

[3] فايز الظفيري، الأحكام العامة للجريمة الإلكترونية، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مصر، السنة الرابعة والأربعون، العدد 2، 2002، ص485.

[4] عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار بهجات للطباعة والتجليد، مصر، ط1، 2009، ص19.

[5] خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص74.

[6] *Redouane Semlali, art-Cit,p.40, voir aussi, Frédérique Chopin, Les politiques publiques de lutte contre la cybercriminalité, Actualité Juridique Pénal, Editions Dalloz, 2009,p101.*

[7] *Nidal El Chaer,Op.Cit,p.20.*

[8] عبد العال الديربي ومحمد صادق إسماعيل، المرجع السابق، ص40.

[9] المرجع نفسه، ص41.

[10] أحمد خليفة الملط، المرجع السابق، ص84.

المعلوماتي، وإنما أيضا من القائمين على ملاحقة هذا النوع من الجرائم، وهذا يضيق على نحو كبير من الجريمة الإلكترونية التي هي في اتساع يوما بعد يوم تبعا لتطور تكنولوجيا المعلوماتية.

من جهة أخرى، هناك جرائم إلكترونية لا تتطلب هذا القدر كله من المعرفة على اعتبار أن المعلوماتية صارت متاحة للجميع مثل: إرسال رسالة نصية بالهاتف أو بالبريد الإلكتروني، أو نسخ بيانات من حاسوب...إلخ، كما أن حصر الجرائم الإلكترونية في موضوع الجريمة والتي تقع فقط على النظام المعلوماتي فيه تضييق بدوره ويندرج تحته نوع واحد من الجرائم الإلكترونية هي المسماة "بجرائم المعالجة الآلية للمعطيات"، إذ يخرج من هذا النطاق جانب كبير من الأفعال غير المشروعة التي يستخدم الحاسب كأداة لارتكابها مثل: جرائم الاحتيال المعلوماتي[1]، وبالتالي يتسم تعريف هذا الاتجاه للجرائم الإلكترونية بالنقصان، مما أدي الى ظهور اتجاه ثان مخالف له نتناوله فيما يأتي.

ثانيا: الاتجاه الموسع لمفهوم الجرائم الإلكترونية: على عكس الاتجاه السابق، يذهب فريق من الفقهاء إلى التوسع في مفهوم الجرائم الإلكترونية أو المعلوماتية وعدم حصرها في الحاسوب وحده أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية، فيعرفونها على أنها " كل فعل إجرامي أو متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة بالمجني عليه، أو كسبا يحققه الفاعل"[2]. كما عرفتها منظمة التعاون الاقتصادي والتنمية *(OCDE)* بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[3]، كما تعرّف أيضا على أنها: "تلك الجرائم المرتكبة ضد الأملاك باستعمال التقنية المعلوماتية"[4].

إن هذه التعريفات واسعة تتيح الإحاطة الشاملة قدر الإمكان بظاهرة جرائم التقنية، كما أنها تعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، كما أنه يتيح إمكانية التعامل مع التطورات التقنية المستقبلية[5]، ويعرفها آخرون على أنها" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[6]، إذ يعتمد هذا التعريف على معيارين : أولهما وصف السلوك، وثانيهما اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها، كما يجمع الفقه

---

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2005، ص30.

[2] حنان ريحان مبارك المضحكي، المرجع السابق، ص26.

[3] أحمد خليفة الملط، المرجع السابق، ص87.

[4] *Alain Bensoussan, L'informatique et le droit, Memento Guide, ,édition Hermes, Paris, France, Tome 1,1994,p.365.*

[5] يونس عرب، جرائم الكمبيوتر والإنترنت المعنى والخصائص والصور واستراتيجية المواجهة القانونية، بحث منشور على الموقع الآتي: *http://www.abhatoo.net.ma*، تاريخ الاطلاع:2015/02/03 على الساعة:13:46، ص14.

[6] نائلة عادل محمد فريد قورة، المرجع السابق، ص30.

الفرنسي بصفة عامة على القول بأن فكرة الغش المعلوماتي *(Fraude Informatique)* التي تعادل جرائم الحاسب الآلي تشمل العديد من الأفعال المتنوعة، حيث عرف كل من الفقيه ميشال *(Michel)* والفقيه ريدو *(Redo)* الجريمة المعلوماتية بأنها" سوء استخدام الحاسب ويشمل الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، وكذا الاستخدام غير المشروع لبطاقات الائتمان وانتهاك ماكينات الحاسب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب وسرقة الحاسب الآلي في حد ذاته أو أي مكون من مكوناته"[1] ، كما عرفت المادة (01) من القانون العربي النموذجي الموحد بشأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصال لسنة 2003 الجرائم الإلكترونية على أنها:" كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني"، وعرفت المادة نفسها الوسيط الإلكتروني على أنه:" شبكة الحاسب الآلي أو الانترنيت أو أي شبكة إلكترونية أخرى"[2]، أو هي:" مجموعة المخالفات التي تقع على شبكات الاتصال عموما وعلى شبكة الإنترنت خصوصا"[3].

وبذلك تمثل هذه التعاريف المفهوم الموسع للجرائم الإلكترونية، والتي تتم بالحاسوب سواء كان هدفا لها أو وسيلة لارتكابها، أو عن طريق شبكة الإنترنت أو بأي وسيلة إلكترونية أخرى تظهر مستقبلا كوسائل الاتصال الحديثة مثل الهاتف النقال وجهاز الفاكس وغيرها.

مما لا شك فيه أن هذا الاتجاه ينطوي على توسع كبير لمفهوم الجرائم الالكترونية، فهي كل جريمة تتم بمساعدة الحاسوب أو في محيطه، أو عن طريق شبكة الإنترنت أو أجهزة الاتصال الحديثة. وبناء على التعريفات السابقة تتخذ الجريمة الإلكترونية صور عديدة، تتمثل في استخدام الحاسوب كوسيلة لارتكاب الجرائم أو الاعتداء على الحاسوب نفسه ونظامه أو استخدام أي وسيلة إلكترونية أخرى توفرها التقنيات الحديثة، بمعنى آخر فإن الجرائم الإلكترونية تزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة، فإذا عدنا للحقيقة الأولى المتصلة بولادة وتطور تقنية المعلومات نجد أن تقنية المعلومات تشمل فرعين جرى بحكم التطور تقاربهما واندماجهما، فرع الحوسبة وفرع الاتصال أما الحوسبة فتقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق، أما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها، هذه الدلالات يحددها الأستاذ زياينغ إكزيوو *(Zhange Yuexiao)* (بالرسائل

---

[1] حنان ريحان مبارك المضحكي، المرجع السابق، ص28.

[2] تم إعداد القانون الاسترشادي العربي الموحد بشأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصال من قبل لجنة مشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب والأمانة العامة لجامعة الدول العربية، وتم إقراره سنة 2003.

[3] *Myriam Quéméner et Yves Charpenel, Op.Cit, p.8*

والأخبار والبيانات والمعرفة والوثائق والأدب والفكر والرموز والعلامات والإرشادات الخفية والأنباء المفيدة والسرية وغير ذلك)[1].

وباستقرائنا لمختلف التعريفات نجد أن تعريف منظمة التعاون الاقتصادي والتنمية السابق الذكر يتسم بالوضوح والشمول وذلك للأسباب الآتية:

– تحديد لماهية السلوك الإجرامي للجريمة، إذ شمل كل من الفعل الإيجابي والسلوك السلبي المتمثل في الامتناع.

–اعتماد تعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة الجرائم التقنية، وذلك لربطه بين الجريمة وأي تدخل للتقنية المعلوماتية بصفة مباشرة أو غير مباشرة كما تتسم هذه التقنية بالتطور المستمر.

– يعبر عن الطابع التقني المميز الذي تنطوي تحته أبرز صور الجريمة الإلكترونية.

–يتيح إمكانية التعامل مع التطورات المستقبلية في مجال تقنية المعلوماتية ونظم الاتصالات.

ونستخلص مما سبق أن اختلاف الفقه في وضع تعريف للجريمة المعلوماتية أو الإلكترونية مرده، الاختلاف في المعيار المعتمد عليه والزاوية التي ينظر إليها كل اتجاه إلى هاته الجريمة المستحدثة، إلا أنه يمكن إعطاء تعريف ملخص تبعا لهذه الاتجاهات فهي:" سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الكمبيوتر" فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الجرمية ومعاقب عليه قانونا، لأن إسباغ الصفة الإجرامية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك، ومحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة ، بيانات ومعلومات معالجة ومخزنة ، البرامج بأنواعها المعلومات المستخرجة ، والمتبادلة بين الأنظمة المعلوماتية...إلخ). وأما الكمبيوتر فهو "النظام التقني بمفهومه الشامل الذي يزاوج بين تقنيات الحوسبة والاتصال" بما في ذلك شبكات المعلومات[2].

وعلى هذا الأساس فإن محاولة إعطاء تعريف لهذا النوع من الجرائم المستحدثة الذي يتم في بيئة افتراضية يجب أن يراعى فيه عدة اعتبارات منها:

1. يجب أن يتلاءم هذا التعريف مع فكرة عالمية المعلومات والاتصالات وأن يكون واضحا عالميا.

---

[1] يونس عرب، جرائم الكمبيوتر، المرجع السابق، ص ص1-2.

[2] يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، ورقة عمل مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط، سلطة عمان، يومي 2 و 4 أفريل، 2006، ص 7.

2. يجب مراعاة التطورات المتلاحقة في عالم الحوسبة والاتصال ويسمح باستيعاب كل ما يستجد من صور للجرائم الإلكترونية.

3. يجب توضيح خصوصية الجرائم الإلكترونية لما تحتويه على أشكال مختلفة للسلوك الإجرامي بحيث يظهرا جليا دور الحاسوب في ارتكاب هذه الجرائم.

مما سبق ذكره يُثار التساؤل الآتي: ما هو موقف المشرع الجزائري بشأن تعريف الجرائم الإلكترونية ؟ وهل اعتمد التعريف الضيق أو الموسع لها؟ هذا ما سنتعرف عليه في الفرع الموالي.

الفرع الثاني: موقف المشرع الجزائري:

نتيجة لما أفرزته الثورة المعلوماتية من أشكال جديدة للإجرام لم يكن للمجتمع سابق عهد بها وعلى غرار كثير من الدول، قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم:04-15 المؤرخ في:10 نوفمبر2004، بإضافة قسم سابع مكرر تحت عنوان" جرائم المساس بأنظمة المعالجة الآلية للمعطيات" من المادة (394 مكرر- 394 مكرر7)، حيث جاء في أسباب هذا التعديل:" إن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى الى بروز أشكال جديدة للإجرام مما دفع بالكثير من الدول إلى النص على معاقبتها، وأن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات وأن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات، وسوف يمكّن لا محالة من مواجهة بعض أشكال الإجرام الجديد"[(1)]. من جانب آخر أقر المشرع الجزائري بمسؤولية الشخص المعنوي وعاقب على الشروع والاتفاق الجنائي، وشدّد من العقوبات في بعض هذه الجرائم ، يذكر أننا سنتطرق في بحثنا هذا إلى جملة القوانين التي أقرها المشرع الجزائري بخصوص مكافحة الجرائم الإلكترونية سواء بموجب القانون العام أو بموجب القانون الخاص.

في هذا الشأن، اصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية أو المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب أحكام المادة (02/أ) من القانون رقم: 04 - 09 مؤرّخ في: 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[(2)] على أنها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية..."، فنص على جرائم

---

[1] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، مصر، 2010 ص27.

[2] القانون رقم: 09 - 04 مؤرّخ في:5 أوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (ج.ر) رقم:47 المؤرخة في:2009/08/16، ص ص5-9.

المساس بأنظمة المعالجة الآلية للمعطيات بموجب المواد من (394مكرر-394مكرر7) من (ق.ع.ج)، وإن كان استعمال هذا المصطلح ينصرف وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكة المعلومات، وهو بذلك يتوافق مع موقف المشرع الفرنسي في أن نظام المعالجة الآلية للمعطيات يشمل أيضا شبكة المعلومات وفقا للقانون الصادر سنة 1978، بمعنى أنه يشمل جميع العمليات التي تتم بواسطة الوسائل الإلكترونية[1]. غير أن هذا المصطلح يقتصر على الجرائم التي تستهدف النظام فقط ليخرج بذلك من نطاقه ما دون ذلك من الجرائم التي يكون فيها نظام المعالجة الآلية للمعطيات وسيلة لارتكابها[2].

وانطلاقا من فحوى هذه المادة نستنتج أن المشرع الجزائري قسم هذه الجرائم المستحدثة الى ثلاثة أنواع:

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات.
- جرائم ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية.
- جرائم ترتكب أو يسهل ارتكابها عن طريق نظام للاتصالات الإلكترونية.

وقصد توضيح المصطلحات، نص في المادة (02/ب) نفسها على تعريف المنظومة المعلوماتية على أنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، والملاحظ أن هذا التعريف يتفق مع نص المادة الأولى من الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي(إ.أ.م.إ.م) ببودابيست لسنة2001 إذ تنص على:" يعتبر النظام المعلوماتي جهاز يتكون من معدات وبرامج قائمة للمعالجة الآلية للبيانات الرقمية...يمكن ان تكون منفردة أو متصلة مع أجهزة مماثلة أخرى داخل شبكة..."[3]، ويتفق أيضا مع نص المادة (5/02) من الاتفاقية العربية لمكافحة

---

[1] عائشة بن قارة مصطفى، المرجع السابق، ص35.

[2] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1 2012، ص36.

[3] مواكبة للتطور الحاصل في مجال تقنية المعلومات، فقد أبرم المجلس الأوروبي اتفاقية ببودابست في: 2001/11/8 تتعلق بمكافحة الإجرام المعلوماتي (إ.أ.م.إ.م)، وضعت للتصديق عليها بتاريخ: 2001/11/23، والتي تضمنت التعريف بأهدافها و وضعت قائمة للجرائم التي يجب على الدول المصادقة عليها وتجريمها في قوانينها الداخلية، حيث وقعت عليها 30دولة. تعد هذه الاتفاقية الأولى في مجال مكافحة جرائم الكمبيوتر والإنترنت تستمد منها معظم التشريعات المقارنة قوانينها الداخلية في مجال مكافحة هذه الجرائم ومنها المشرع الجزائري. نصت هذه الاتفاقية على العديد من الجرائم منها: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، التزوير المعلوماتي إجراءات جمع الدليل الإلكتروني، الإباحية الالكترونية...إلخ. وتعمد الاتفاقية إلى تنسيق القوانين الجديدة في دول عديدة. جاءت نتيجة مشاورات طويلة بين الحكومات وأجهزة الشرطة وقطاع الكمبيوتر، وصاغ نصها عدد من الخبراء في مجلس أروبا بمساعدة عدة دول منها الولايات المتحدة. كما تحدد الاتفاقية أفضل الطرق الواجب اتباعها للتحقيق في جرائم الإنترنت، والتي تعهدت الدول الموقعة بالتعاون الوثيق من أجل محاربتها. كما تحاول الاتفاقية الموازنة بين جهات المتابعة وصلاحياتها وبين احترام حقوق الإنسان ومصلحة==

جرائم تقنية المعلومات(إ.ع.م.ج.ت.م) المحرّرة بالقاهرة بتاريخ:12/21 /2010، والتي صادقت عليها الجزائر بتاريخ:2014/09/08[1]. حيث عرّفت النظام المعلوماتي على أنه:" مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات".

وفي الشأن نفسه، نصت المادة (02/ج) من القانون رقم: 09-04 سالف الذكر على تعريف الاتصالات الإلكترونية على أنها:" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية" وتندرج تحت ذلك كافة الوسائل الإلكترونية المستخدمة للتحكم في المعلومات وتجميعها ومعالجتها واختزانها واسترجاعها ونقلها وتبادلها وإتاحة الوصول إليها في كل وقت بشكل إلكتروني كالحاسوب، الهاتف النقال، الفاكس أجهزة اللاسلكي...إلخ[2]، ويعتبر هذا مجالا خصبا لارتكاب الجرائم الإلكترونية.

وبالرجوع أيضا إلى نصوص قانون العقوبات نجد أن المشرع الجزائري وقصد التوسع في سياسته الجنائية لمكافحة هذا النوع المستحدث من الجرائم الإلكترونية نص في المادة (144مكرر) على:" يعاقب بالحبس...كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأي آلية لبث الصوت والصورة أو بأي وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى"، والأمر نفسه نصت عليه المادة (146) حينما ترتكب هذه الجرائم باستعمال الوسائل المذكورة في المادة (144مكرر) ضد البرلمان والمجالس القضائية والمحاكم وضد الجيش وأي هيئة نظامية.

==مستخدمي ومزودي الخدمة، إذ جاء في ديباجتها ما يلي: " اقتناعا من الدول أعضاء مجلس الاتحاد الأوروبي بضرورة منح الأولوية للسعي من أجل تنفيذ سياسة جنائية مشتركة تهدف إلى حماية المجتمع من أخطار جرائم الإنترنت، عن طريق تبني التشريع المناسب ودعم التعاون الدولي وإدراكا لعمق التغيرات التي أحدثها التحول إلى الرقمية وارتباط شبكات الكمبيوتر مع بعضها البعض مع استمرار عولمتها وانشغالا بمخاطر احتمال استخدام شبكات الكمبيوتر والمعلومات الإلكترونية في ارتكاب جرائم جنائية ..."راجع:

Myriam Quéméner et Joel Ferry,Op.Cit,pp.270-272.

Frédérique chopin,art-cit,p.102.

لأكثر تفاصيل، يرجى الاطلاع على نصوص الاتفاقية المنشورة على الموقع الرسمي للمجلس الأوروبي على شبكة الإنترنت على الرابط الآتي:

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008156d، تاريخ الاطلاع:2015/12/11 على الساعة:07:49، ص ص1-24.

[1] المرسوم الرئاسي رقم:14-252 المؤرخ في:2014/09/08، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ: 2010/12/21، (ج.ر) رقم:57 المؤرخة في:2014/09/28، ص ص04-14، حيث تهدف هذه الاتفاقية في مادتها الأولى إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

[2] رشيدة بوكر، المرجع السابق، ص37.

فقد تتم الجريمة بواسطة الكمبيوتر سواء كان وسيلة أو هدفا وباستعمال شبكة الإنترنت، أو بواسطة الهاتف النقال خاصة النوع الذكي الذي يستطيع الاتصال بشبكة الإنترنت، أو عن طريق اللوحة الرقمية *(Tablette)* المزودة بشريحة ذكية، أو أي وسيلة أخرى متوفرة، كما قام في سياسته الجنائية بتوسيع مكافحته للجرائم الإلكترونية بإضفاء الحماية الجزائية على وسائل الدفع الإلكتروني بموجب المواد من(93 مكرر2-93مكرر5) من القانون رقم: 08-01 المؤرخ في:2008/01/23 يعدل ويتمم القانون رقم:83-11 المؤرخ في:1983/07/02 المتعلق بالتأمينات الاجتماعية[1]، والتي تنص على الجرائم الإلكترونية المتعلقة بسوء استخدام البطاقة الإلكترونية للمؤمن له اجتماعيا مثل: تعديل وحذف المعطيات والاستعمال غير المشروع للمفتاح الإلكتروني لهيكل العلاج، وعزّز من هذا الاتجاه بموجب القانون رقم:2000-03 المؤرخ في:2000/08/05 يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية بموجب المواد(127و135و136و137)، وهي حماية جزائية مهمة أضفاها المشرع على إساءة استخدام هذه الوسيلة الإلكترونية.

وبالتالي حاول المشرع التوسّع في إعطائه لمفهوم الجرائم الإلكترونية التي تتم بوسائل متعددة كاستعمال الحاسوب وشبكة الإنترنت والهاتف النقال واللاسلكي وأي وسيلة إلكترونية أو معلوماتية تظهر في المستقبل، وبالتالي ساير المشرع التطورات المذهلة الحاصلة في مجال الحوسبة والاتصالات، وما يعزّز هذا الاتجاه الموسّع لمفهوم الجرائم الإلكترونية، هو قيامه بالتصديق على (إ.ع.م.ج.ت.م) المشار إليها سابقا، والتي تنص على جرائم جديدة كجريمة الاحتيال والتزوير الإلكتروني والإباحية باستخدام تقنية المعلومات والاعتداء على حرمة الحياة الخاصة، والاستخدام غير المشروع لأدوات الدفع الإلكتروني والمساعدة القضائية المتبادلة، وتسليم المجرمين...إلخ، والتي سيترجمها المشرع الجزائري بموجب نصوص قانونية لاحقة تضاف إلى المنظومة القانونية الحالية لمكافحة هذه الجرائم المستحدثة.

فمن خلال استعمال المشرع الجزائري لهذا المصطلح " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" للدلالة على الجرائم الالكترونية فهو يزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة فالحوسبة تقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة البيانات، أما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها[2].

---

[1] المادة (93 مكرر2 - 93 مكرر5) من القانون رقم: 08-01 المؤرخ في:2008/01/23، يتمم القانون رقم:83-11 المؤرخ في:1982/07/02 والمتعلق بالتأمينات الاجتماعية، (ج. ر) رقم:04 المؤرخة في:2008/01/27، ص ص4-6.

[2] يونس عرب، جرائم الكمبيوتر، المرجع السابق، ص1.

وعليه فان غاية هذا البحث، هو الإحاطة بمجمل السياسة الجنائية للمشرع الجزائري في شقّيها الموضوعي والإجرائي في مجال مكافحة الجرائم الإلكترونية التي تتم في هذه البيئة الافتراضية، والتي تستعمل الحاسوب وشبكة الإنترنت ونظم الاتصالات الإلكترونية أو أي وسيلة تقنية تظهر مستقبلا على اعتبار أن هذه الجرائم تتم في بيئة إلكترونية بغض النظر عن الوسيلة المستخدمة، فلقد وفّق المشرع الجزائري في اختياره مصطلح" الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" التي تتوافق مع مصطلح "الجرائم الإلكترونية" بالمفهوم الواسع والذي استعملناه في بحثنا هذا، وذلك للأسباب الآتية:

●إن الجرائم الناشئة في البيئة الرقمية جرائم حديثة يرتبط مفهومها بظهور التكنولوجيا الحديثة وما يواكبها من تطور مستمر في تشغيل ونقل وتخزين المعطيات في شكل إلكتروني، فهي تشمل أجهزة الحاسوب ووسائل الاتصال وشبكات الربط وغيرها، مما يجعل المصطلح المعبّر عنها يتسم بالمرونة ويسمح باستيعاب تكنولوجيا المعلومات والمبتكرات والتقنيات الراهنة والمستقبلية، وهو ما يتحقق فعلا مع مصطلح: "الجرائم الالكترونية".

●ان استعمال هذا المصطلح له مفهوم واسع، فهو يشمل كل الاعتداءات التي تتم في بيئة افتراضية بما فيها الجرائم التي تقع على نظم المعالجة الآلية للمعطيات أو تكون وسيلة لارتكابها، كما يشمل جميع الابتكارات الإلكترونية في مجال تكنولوجيا المعلومات والاتصالات[1].

●يعبر هذا المصطلح عن الطابع التقني والمميز للجرائم الإلكترونية، وتقع تحته أبرز صورها كما يساعد في التعامل مع التطورات المستقبلية لتقنيات الحوسبة والاتصال.

المطلب الثاني: تصنيف الجرائم الإلكترونية وأنواع المجنى عليهم

تطرقنا سلفا إلى تعريف الجريمة الإلكترونية، وما نتج عن ذلك من صعوبات جمة بدأ بالاختلاف في استعمال مصطلح موحد للدلالة عليها إلى تعدد الاتجاهات الفقهية في محاولة وضع تعريف لها، وهو اختلاف رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات والاتصالات، وطالما أن الجرائم الإلكترونية ليست فئة واحدة أو نوعا واحدا، فإن التصنيفات هي الأخرى ليست نوعا واحدا واختلفت باختلاف أنواع الجرائم الإلكترونية.

وعلى هذا الأساس فإن الجرائم الإلكترونية في نطاق الظاهرة الإجرامية المستحدثة، جرائم تنصب على معطيات الحاسوب (بيانات ومعلومات وبرامج ونظم معلوماتية...إلخ) وتطال الحق في المعلومات، ويستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسوب بوصفه نظاما حقق التزاوج بين

---

[1] رشيدة بوكر، المرجع السابق، ص37.

تقنيات الحوسبة والاتصالات، وبرغم ذلك سنحاول الوقوف على أبرز هذه التصنيفات إضافة الى أنواع المجنى عليهم في هذا النوع المستحدث من الجرائم قصد إبراز معالم وسمات السياسة الجنائية للمشرع الجزائري في هذا المجال، لذا سنتطرق إلى تصنيف الجرائم الإلكترونية تبعا لعدة معايير في (الفرع الأول)، ثم نتناول أنواع المجني عليهم في (الفرع الثاني).

الفرع الأول: تصنيف الجرائم الإلكترونية:

يصنف الفقهاء والدارسون جرائم الكمبيوتر والإنترنت ضمن فئات متعددة، تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني، فبعضهم يقسمها إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته، وبعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء، وكذا تعدد الحق المعتدى عليه فتوزع جرائم الحاسوب وفق هذا التقسيم إلى جرائم تقع على الأموال بواسطة الحاسوب وتلك التي تقع على الحياة الخاصة[1]. ومن الملاحظ أن هذه التقسيمات لم تراعي بعض خصائص هذه الجرائم وموضوعها، والحق المعتدى عليه لدى وضعها لأساس أو معيار التقسيم. وعليه ونظرا لطبيعة هذا النوع المستحدث من الجرائم تعددت تصنيفاتها بتعدد معايير التصنيف، سنتطرق إلى بعضها فيما يأتي:

أولا: تبعا لنوع المعطيات ومحل الجريمة: رافق هذا التصنيف مع جملة التشريعات في مجال تقنية المعلومات، وهو يعكس أيضا التطور التاريخي لظاهرة الجرائم الإلكترونية والإنترنت ونجد هذا التصنيف سائدا في مختلف مؤلفات الفقيه الألماني أولريش سايبر *(Ulrich Sieber)* والمؤلفات المتأثرة به[2]، ولهذا تقسم جرائم الكمبيوتر وفق هذا المعيار إلى :

أ–الجرائم الماسة بقيمة معطيات الحاسوب: ويضم هذا القسم فئتين هما: الأولى الجرائم الواقعة على ذات المعطيات، كجرائم الاتلاف والتشويه للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام البرامج الخبيثة كالفيروسات. والثانية الجرائم الواقعة على ما تمثله المعطيات المعالجة آليا من أموال أو أصول، كجرائم غش الحاسوب التي تستهدف الحصول على المال أو جرائم الاتجار بالمعطيات، وجرائم التلاعب في المعطيات المخزنة داخل نظم الحاسوب واستخدامها مثل: تزوير المستندات المعالجة آليا[3].

---

[1] عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، دار المستقبل للنشر والتوزيع، الأردن، ط1، 2009 ، ص131.

[2] يوسف حسن يوسف، الجريمة الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر، ط1، 2011، ص37.

[3] يوسف المصري، المرجع السابق، ص27.

ب-الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة: وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة[1].

ج-**الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات):** في هذا المجال لا يجب الخلط بين الاعتداء على الملكية الأدبية والفكرية التي تنصب على البرامج والمعلومات، وبين الاعتداء على الحقوق الفكرية التي تقع على العناصر غير المادية لنظام المعلوماتية[2]، وتشمل نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص واستغلالها ماديا والاعتداء على العلامة التجارية وبراءة الاختراع...إلخ[3]. حيث تشكل قرصنة برامج الحاسوب خسائر كبيرة لاقتصاديات الدول، إذ يقدر تحالف الأعمال البرمجية بأن 36% من البرمجيات المحملة للحواسيب حول العالم في سنة 2003 مقرصنة، مما يمثل خسارة تقدر بحوالي 290 مليار دولار[4].

ثانيا: تبعا لدور الكمبيوتر في الجريمة: تطرقنا في مطلب سابق إلى دور الكمبيوتر في الجريمة، وخلصنا أنه قد يكون هو نفسه هدفا للاعتداء، بمعنى أن يستهدف الفعل المجرم المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة الكمبيوتر والشبكات، وهذا ما يعبّر عنه بالمفهوم الضيق للجرائم الإلكترونية، وقد يكون الكمبيوتر وسيلة مثل: الاحتيال ببطاقات الائتمان أو التزوير، كما قد يكون الحاسوب جسرا لارتكاب جرائم أخرى كالمتاجرة بالمخدرات وغسيل الأموال والإباحية الإلكترونية [5]. كما قد يكون الكمبيوتر مخزنا للمادة الجرمية.

في هذا الصدد ينتج عن دور الكمبيوتر في الجريمة مفهومين هم: الأول يتعلق بجرائم التخزين بمعنى تخزين المواد الجرمية المستخدمة في ارتكاب الجريمة أو الناشئة عنها، والثاني يتعلق بجرائم المحتوى أو ما يعبر عنه بالمحتوى غير المشروع، والاصطلاح الأخير استخدم في ضوء تطور

---

[1] علي عبود جعفر، المرجع السابق، ص88.

[2] أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي-دراسة مقارنة، دار النهضة العربية، القاهرة، مصر،2000، ص212.

[3] يونس عرب، صور الجرائم، المرجع السابق، ص9.

[4] داريل بانثيير، استمرار القرصنة تبعاتها على الإبداع وعلى الثقافة وعلى التنمية المستدامة، نشرة حقوق الملكية، جويلية 2005، بحث منشور على الموقع الرسمي لمنظمة اليونسكو على الرابط الآتي:
https://www.google.com/url?q=http://portal.unesco.org/culture/es/files/29853/11467333771bull_3_2005_ar.pdf/bull_3_2005_ar.pdf&sa=U&ved=0ahUKEwjk-XM37TPAhWE1RoKHaldCUYQFggEMAA&client=internal-uds-cse&usg=AFQjCNHwg1ANz88pxIufSbBFaymwJLj8FQg، تاريخ الاطلاع:2016/09/24 على الساعة:18:18، ص6.

[5] عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن ط1، 2011، ص123.

أشكال الجريمة مع استخدام الإنترنت، وأصبح المحتوى غير القانوني يرمز إلى جرائم المقامرة ونشر المواد الإباحية والغسيل الإلكتروني للأموال وغيرها، باعتبار أن مواقع الإنترنت تتصل بشكل رئيس بهذه الأنشطة[1]. إن هذين المفهومين يتصلان بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة وفي الوقت نفسه كوسيلة لارتكابها، وتبعا له تنقسم جرائم الكمبيوتر إلى جرائم تستهدف نظام المعلوماتية نفسه كالاستيلاء على المعلومات واتلافها أو تعديلها، وجرائم ترتكب بواسطة نظام الكمبيوتر نفسه كجرائم احتيال الكمبيوتر[2] .

كان من نتائج الاتجاه العالمي الجديد في ضوء تطوير التدابير التشريعية في أوروبا تحديدا أن قسّم هذه الجرائم إلى جرائم هدف ووسيلة ومحتوى، وأفضل ما يعكس هذا التقسيم اتفاقية بودابست لجرائم الكمبيوتر والإنترنت لسنة 2001، حيث اتجهت الجهود إلى وضع إطار عام لتصنيف جرائم الكمبيوتر والإنترنت، وعلى الأقل وضع قائمة تمثل الحد الأدنى محل التعاون الدولي في مجال مكافحة هذه الجرائم. حيث أثمرت جهود دول أوروبا وبمساهمة كل من أستراليا وكندا وأمريكا وضع إطار لتقسيم جرائم الكمبيوتر والإنترنت، مع ملاحظة أنها تستثني من هذا التقسيم جرائم الخصوصية لوجود اتفاقية أوروبية مستقلة لسنة 1981 تعالج حماية البيانات الاسمية من مخاطر المعالجة الآلية للبيانات[3].

لقد أوجدت اتفاقية بودابست لسنة 2001 تصنيفا جديدا نسبيا، فقد تضمن أربعة أقسام رئيسة لجرائم الكمبيوتر والإنترنت نوجزها كما يأتي[4]:

1- الجرائم التي تستهدف عناصر السرية والسلامة وديمومة توفر المعطيات والنظم: وتشمل الدخول غير قانوني وتدمير المعطيات واعتراض النظم...إلخ.

2- الجرائم المرتبطة بالكمبيوتر: مثل التزوير المعلوماتي.

3- الجرائم المرتبطة بالمحتوى : وتضم صنفا واحدا وهي الجرائم المتعلقة بالأفعال الإباحية واللاّأخلاقية .

4- الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة: مثل قرصنة البرمجيات .

---

[1] يونس عرب، صور الجرائم، المرجع السابق، ص10.

[2] علي عبود جعفر، المرجع السابق، ص89.

[3] عبد الصبور عبد القوي علي مصري، الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، القاهرة، مصر، ط1، (ب.س.ط) ص23.

[4] يوسف حسن يوسف، المرجع السابق، ص40.

ثالثا: تبعا لمساسها بالأشخاص والأموال : يوجد هذا التصنيف في الدراسات والأبحاث الأمريكية، وأبرز تقسيم في هذا الصدد ذلك الذي تضمنه مشروع القانون النموذجي لجرائم الكمبيوتر والإنترنت لسنة 1998 من قبل فريق بحثي أكاديمي أطلق عليه إسم: (*Model State Computer Crimes Code)*، أين تم تقسيم جرائم الكمبيوتر والإنترنت إلى الجرائم الواقعة على الأشخاص كجرائم الآداب، والجرائم الواقعة على الأموال مثل: الاحتيال والتزوير المعلوماتي والمقامرة...إلخ. ويلاحظ أن التقسيم يقوم على فكرة الغرض النهائي أو المحل النهائي الذي يستهدفه الاعتداء، لكنه ليس تقسيما منضبطا ولا هو تقسيم محدد الأطر، فالجرائم التي تستهدف الأموال تضم من حيث مفهومها السرقة والاحتيال فقط، أما الجرائم التي تستهدف التزوير فتمس الثقة والاعتبار والجرائم الواقعة ضد الآداب قد تتصل بالشخص وقد تتصل بالنظام والأخلاق العامة[1]. وحسب هذا القانون تصنف جرائم الكمبيوتر على النحو الآتي:

أ- **قسم الجرائم التي تستهدف الاشخاص:** وتضم قسمين رئيسين هما[2]:

- **قسم الجرائم غير الجنسية التي تستهدف الاشخاص:** وتشمل جرائم ضد شخصية الفرد وممتلكاته، والقتل بالكمبيوتر والتسبب بالوفاة وجرائم الإهمال المرتبط بالكمبيوتر، والتحريض على الانتحار، والتحريض القصدي للقتل عبر الإنترنت، والتحرش والمضايقة عبر وسائل الاتصال المؤتمتة وأنشطة اختلاس النظر أو الاطلاع على البيانات الشخصية، وقنابل البريد الإلكتروني والدخول غير المصرح به...إلخ[3].

- **قسم الجرائم الجنسية:** وتشمل تحريض القاصرين على أنشطة جنسية غير مشروعة وإفسادهم بأنشطة جنسية عبر الوسائل الإلكترونية، وإغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة، وتلقي أو نشر المعلومات عن القاصرين عبر الكمبيوتر من أجل أنشطة جنسية غير مشروعة، والتحرش الجنسي بالقاصرين عبر الكمبيوتر والوسائل التقنية ونشر وتسهيل نشر واستضافة المواد الفاحشة عبر الإنترنت بوجه عام وللقاصرين بوجه خاص، ونشر الفحش والمساس بالحياء، واستخدام الإنترنت لترويج الدعارة بصورة قسرية، والحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة غير مشروعة. وهي أوصاف تجتمع جميعا تحت صورة واحدة هي استغلال الإنترنت والكمبيوتر لترويج الدعارة أو إثارة الفحش واستغلال الأطفال والقصر في أنشطة جنسية غير مشروعة[4].

---

1 يوسف أبو الحجاج، المرجع السابق، ص42.

2 يوسف حسن يوسف، المرجع السابق، ص42.

3 عادل عزام سقف الحيط، المرجع السابق، ص126.

4 يوسف أبو الحجاج، المرجع السابق، ص43.

ب- قسم الجرائم التي تستهدف الأموال: باستثناء جريمة السرقة، تشمل هذه الطائفة أنشطة الدخول أو التواصل غير المصرح به مع نظام الكمبيوتر أو الشبكة، إما مجردا أو لجهة ارتكاب فعل آخر ضد البيانات والبرامج والمخرجات، وتخريب المعطيات والنظم، وخلق البرمجيات الخبيثة والضارة، ونقلها عبر النظم والشبكات، واستخدام إسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص، وادخال معطيات خاطئة أو مزورة إلى نظام الكمبيوتر، والتعديل غير المصرح به لأجهزة ومعدات الكمبيوتر، والاتلاف غير المصرح به لنظم الكمبيوتر، وتعطيل أو اعتراض عمل النظام أو الخدمات، وأنشطة الاعتداء على الخصوصية (جرائم الاختراق)، وإفشاء كلمة سر الغير والحيازة غير المشروعة للمعلومات، وإساءة استخدام المعلومات، ونقل معلومات خاطئة[1] .

- **جرائم الاحتيال والسرقة:** وتشمل جرائم الاحتيال عن طريق التلاعب بالمعطيات والنظم واستخدام الكمبيوتر للحصول على أو استخدام البطاقات المالية للغير دون ترخيص، والاختلاس عبر الكمبيوتر أو بواسطته، وسرقة معلومات الكمبيوتر وقرصنة البرامج وسرقة خدمات الكمبيوتر، وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر.
- **جرائم التزوير:** وتشمل تزوير البريد الإلكتروني والوثائق والسجلات المتعلقة بالهوية.
- **جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب:** وتشمل تملك وإدارة مشروع مقامرة على الإنترنت وتشجيعه وتسهيل إدارته، واستخدام الإنترنت لترويج الكحول ومواد الإدمان للقصر.
- **جرائم الكمبيوتر ضد الحكومة:** وتشمل هذا القسم كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون، والإخفاق في الابلاغ عن جرائم الكمبيوتر، والحصول على معلومات سرية، والإخبار الخاطئ عن جرائم الكمبيوتر، والإرهاب الإلكتروني[2] .

رابعا: تصنيف الجرائم الإلكترونية كجرائم كمبيوتر وجرائم إنترنت: تبعا للتطورات المذهلة الحاصلة في مجال الحوسبة والاتصال، فإنه من الطبيعي أن يكون ثمة مفهوم لجرائم ترتكب على الكمبيوتر وبواسطته قبل أن يشيع استخدام شبكات المعلومات وتحديدا الإنترنت، ومن الطبيعي أن تخلق الإنترنت أنماطا جرمية مستحدثة، أو أن تؤثر بالآلية التي ترتكب فيها جرائم الكمبيوتر ذاتها بعد أن تحقق توصيل الحواسيب معا في نطاق شبكات محلية وإقليمية وعالمية، أو على الأقل تطرح أنماط فرعية من الصور القائمة تختص بالإنترنت ذاتها. ومن هنا جاء هذا التقسيم ، وسنجد أنه وإن كان مبررا من حيث المنطلق، فإنه غير صحيح في الوقت الحاضر بسبب سيادة مفهوم نظام الكمبيوتر

---

[1] عبد الحكيم رشيد توبة، المرجع السابق، ص136.

[2] يوسف المصري، المرجع السابق، ص ص32-33.

المتكامل الذي لا تتوفر حدود وفواصل في نطاقه بين وسائل الحوسبة (الكمبيوتر) ووسائل الاتصال (الشبكات)[1].

وفي نطاق هذا المعيار يجري التمييز بين الأفعال التي تستهدف المعلومات في نطاق نظام الكمبيوتر ذاته – خلال مراحل المعالجة والتخزين والاسترجاع – وبين الأنشطة التي تستهدف الشبكات ذاتها أو المعلومات المنقولة عبرها، والأنشطة التي تستهدف مواقع الإنترنت وخوادمها من نظم الكمبيوتر الكبيرة والعملاقة، أو تستهدف تطبيقات واستخدامات وحلول الإنترنت وما نشأ في بيئتها من أعمال وخدمات إلكترونية[2]. من جانب آخر، يحصر البعض أنشطة جرائم الإنترنت بتلك المتعلقة بالاعتداء على المواقع وتعطيلها أو تشويهها أو تعطيل تقديم الخدمة، وكذلك أنشطة المحتوى الضار، كترويج المواد الإباحية والمقامرة، وأنشطة إثارة الأحقاد والتحرش والإزعاج والابتزاز...إلخ إضافة إلى مختلف الأنشطة التي تستخدم البريد الإلكتروني والمراسلات الإلكترونية وغرف الحوار وأنشطة الاستيلاء على كلمات سر المستخدمين والهوية ووسائل التعريف، وأنشطة الاعتداء على الخصوصية عبر جمع المعلومات من خلال الإنترنت، وأنشطة احتيال الإنترنت مثل: الاحتيال في المزادات وعدم التسليم الفعلي للمنتجات والخدمات، وأنشطة نشر الفايروسات والبرامج الخبيثة عبر الإنترنت...إلخ[3].

أما بخصوص جرائم الكمبيوتر، فإنها وفق هذا التقسيم ترجع إلى الأنشطة التي تستهدف المعلومات والبرامج المخزنة داخل نظم الكمبيوتر، وتحديدا أنشطة التزوير واحتيال الكمبيوتر وسرقة المعطيات وسرقة وقت الآلة واعتراض المعطيات خلال النقل برغم اتصال هذا المفهوم بالشبكات أكثر من نظم الكمبيوتر، إضافة للتدخل غير المصرح به والذي يتوزع ضمن هذا التقسيم بين دخول غير مصرح به لنظام الكمبيوتر ودخول غير مصرح به للشبكات فيتبع لمفهوم جرائم الإنترنت[4].

يعتبر هذا التقسيم غير دقيق ومخالف للمفاهيم التقنية وللمرحلة التي وصل إليها تطور وسائل تقنية المعلومات وعمليات التكامل والدمج بين وسائل الحوسبة والاتصال، فمن جهة ثمة مفهوم عام لنظام الكمبيوتر يستوعب كافة مكوناته المادية والمعنوية المتصلة بعمليات الإدخال والمعالجة والتخزين والتبادل، مما يجعل الشبكات وارتباط الكمبيوتر بالإنترنت جزءا من فكرة تكاملية النظام، ومن جهة أخرى، فإن أنشطة الإنترنت تتطلب أجهزة كمبيوتر تنجز بواسطتها، وهي تستهدف

[1] يونس عرب، صور الجرائم، المرجع السابق، ص13.

[2] عادل عزام سقف الحيط، المرجع السابق، ص ص122-123.

[3] يونس عرب، صور الجرائم، المرجع السابق، ص13.

[4] عبد الصبور عبد القوي علي مصري، المرجع السابق، ص30.

أيضا معلومات مخزنة أو معالجة ضمن أجهزة كمبيوتر، وهي الخوادم التي تستضيف مواقع الإنترنت أو تديرها. وعليه يعتبر هذا المعيار غير صحيح إذا عمدنا إلى تحليل كل نمط من أنماط الجرائم المتقدمة في ضوء هذا المعيار، فمثلا تعد جريمة الدخول غير المصرح به لنظام الكمبيوتر وفق هذا المعيار جريمة كمبيوتر، أما الدخول غير المصرح به الى موقع إنترنت فإنها جريمة إنترنت ، مع أن الحقيقة التقنية تبين أن الدخول في الحالتين هو دخول إلى نظام الكمبيوتر عبر الشبكة [1].

تقدير:

تناولنا أهم نظريات تصنيف الجرائم الإلكترونية أو المعلوماتية، ومن خلال ما سبق يمكن القول أن أكثر التقسيمات انضباطية، هو معيار تصنيف هذه الجرائم تبعا لدور الكمبيوتر في الجريمة، سواء كان هدفا للجريمة كاستهداف نظامه بهدف تعديل المعلومات أو الاستيلاء عليها أو اتلافها، أو كان وسيلة للقيام بالجرائم، كجرائم التزوير واحتيال الكمبيوتر. إن الفائدة من هذا التصنيف هو بحث المشرع في سياسته الجنائية سواء المتعلقة بالتجريم أو العقاب، أو بالإجراءات عن كيفية مواجهة هذا النوع المستحدث من الجرائم من خلال تحديد الأفعال المجرمة وشروطها وأركانها وظروفها وتوقيع العقاب عليها، والإجراءات الخاصة بها في مجال البحث والتحري والتفتيش والحجز، وهذا دون الاخلال بمبدأ الشرعية الجزائية.

وهذا ما قام به المشرع الجزائري من خلال تعديل قانون العقوبات بالقانون رقم:04-15 المؤرخ في:10 نوفمبر2004، بإضافة قسم سابع مكرر تحت عنوان" جرائم المساس بأنظمة المعالجة الآلية للمعطيات" من المادة (394 مكرر- 394 مكرر7)، أين نص على مجموعة من الجرائم يكون فيها الكمبيوتر أحيانا هدفا للجريمة وأحيانا أخرى وسيلة لارتكابها، كما يمكن أن يكون بيئة لاحتضان المحتوى المجرم أو غير المشروع، ومثال ذلك: جريمة الدخول عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، جريمة تخريب نظام اشتغال المنظومة، جريمة إدخال عن طريق الغش معطيات في نظام المعالجة الآلية للمعطيات، وجريمة تجميع وتصميم أو بحث أو نشر أو الاتجار في المعطيات المخزنة أو المعالجة آليا...إلخ. وللسبب نفسه نص في القانون رقم: 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على جملة من الإجراءات الخاصة بمكافحة هذه الجرائم خاصة ما تعلق بإجراء تفتيش المنظومة المعلوماتية والحجز عليها واعتراض المراسلات... إلخ.

---

[1] يوسف المصري، المرجع السابق، ص35.

من جهة أخرى، صادقت الجزائر بتاريخ:2014/09/28 على (إ.ع.م.ج.ت.م)، والتي نصت على مجموعة جديدة من جرائم الإنترنت مثل: جريمة التزوير وجريمة الاحتيال وجريمة الإباحية والجرائم المرتبطة بها...إلخ.

وبالتالي نستطيع القول أن المشرع الجزائري تماشى مع الاتجاه العالمي الذي يعكس هذا التصنيف محاولة منه وضع سياسة جنائية فعّالة لمكافحة هذا النوع المستحدث من الجريمة كما سنرى لاحقا.

الفرع الثاني: أنواع المجنى عليهم في الجرائم الإلكترونية:

نتج عن سوء استخدام تقنية المعلومات، جرائم متنوعة تقع على ضحايا تمثل فئات عديدة سواء كانوا أشخاصا معنويين كالجهات الحكومية والمؤسسات المالية والعسكرية أو كانوا أشخاصا طبيعيين.

أولا: الجهات الحكومية والمؤسسات المالية والعسكرية: رغم ما تبذله هذه الهيآت من جهود معتبرة لتوفير الحماية الفنية لأنظمتها المعلوماتية وقواعد بيانتها، إلا أنها تظل عرضة لعمليات القرصنة.

أ- الجهات الحكومية والمؤسسات المالية: تعتبر المؤسسات المالية كالبنوك والشركات المالية وسواء كانت عامة أو خاصة، من أكثر الفئات المستهدفة من قبل مرتكبي الجرائم الإلكترونية نظرا لما تملكه من أموال، واعتمادها على خدمات الحاسوب وشبكة الإنترنيت[1]، فتتعرض مثلا إلى جرائم الاستيلاء على حسابات العملاء، واستعمال بطاقات ائتمان مزورة، وقرصنة البيانات والبرمجيات والأفلام والموسيقى...إلخ[2] مما عرضها لخسائر مادية كبيرة[3]، إضافة الى قطاعات المال تزداد رقعة الجريمة لتشمل شركات التأمين، فلقد شهدت ولاية "لوس أنجلوس الأمريكية "أشهر هذه الجرائم، وذلك

---

[1] خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص150.

[2] جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية، المرجع السابق، ص77. وأيضا، داريل بانثيير، المرجع السابق، ص ص3-5.

[3] في هذا الشأن، أصدر مركز شكاوي جرائم الإنترنت *(the internet crime complaint center)* والمعروف اختصارا ب*(IC3)*، وهو الجهة الرسمية لمراقبة جرائم شبكة الإنترنت في الولايات المتحدة، تقريرا يهدف إلى المنع والحد من انتشار وتأثير جرائم شبكة الإنترنت وتسليط الضوء عليها، ودعم ضباط إنفاذ القانون في تحقيقاتهم. ففي عام 2013، تم معالجة 262813 شكوى ، وهو ما يمثل أكثر من 781.000.000 مليون دولار من الخسائر. كما أشار التقرير إلى دور وكالات إنفاذ القانون وتفاعلهم مع المركز لدعم مبادرات التحقيق الجارية مع التطورات الجديدة في مجال الجريمة السبرانية. حيث أسفرت هذه التحقيقات عن اعتقالات ومضبوطات وإدانات، كما أصدرت *(IC3)* تقارير شهرية وتحليل الاتجاهات وإعلانات الخدمة العامة، والتنبيهات حول جرائم الاحتيال، وغيرها. وسيظل المركز يقدم باستمرار خدماته في مجال التكنولوجيا وضمان تلبية احتياجات جهات إنفاذ القانون، للاستفادة أكثر، يرجى الاطلاع على محتوى التقرير المنشور على الموقع الرسمي لـ:*(IC3)* على الرابط الآتي:*https://pdf.ic3.gov/2013_IC3Report.pdf* ، تاريخ الاطلاع::2015/04/01 على الساعة:09:54.

حينما تمكن أحد موظفي شركة تأمين كبرى من الدخول إلى نظامها الحاسوبي وإضافة عملاء وهميين مؤمّن عليهم، وتمكّن من بيع (46.000) بوليصة تأمين إلى شركة أخرى[1] .

ب- المؤسسات العسكرية: لم تقتصر ثورة المعلومات الحديثة على الجانب المدني فقط، بل امتدت إلى الجانب العسكري، وأدت إلى ظهور ما يسمى "بحرب المعلومات" بين الدول، فالدولة التي تملك المعلومات هي الدولة الأقوى إعمالا لمبدأ: "من يمتلك المعلومة يمتلك السلطة"، فهذه الجرائم هي الأخطر من نوعها نظرا لمساسها بالأمن القومي للدول، فظهرت جرائم التجسس العسكري باستعمال أحدث تقنيات الحوسبة والاتصال، كالحواسيب الخارقة *(Super Computer)*[2]، والأقمار الصناعية الموجهة لأغراض عسكرية...إلخ. نتج عن عمليات التجسّس ما يعرف بالحروب الإلكترونية بين الدول التي تعتمد أساسا على برامج كمبيوتر ذكية ومتطورة جدا، للحصول على معطيات عسكرية حسّاسة كعدد أفراد الجيش وأماكن انتشاره، ونوعية تسليحه، والمواقع العسكرية السرية...إلخ. في هذا الشأن تجدر الإشارة إلى الهجمات الإلكترونية التي تعرضت لها المنشآت النووية الإيرانية في سنة 2010 ، وكان الهدف من ذلك هو التجسّس العسكري وتخريب هذه المنشآت وبالتالي تعطيل برنامج إيران النووي.

ثانيا: الأشخاص الطبيعية: لا يقتصر تصنيف ضحايا الجرائم الإلكترونية على المؤسسات المالية والعسكرية فقط، بل تعداه أيضا إلى الأشخاص الطبيعية، وبالتالي فالكثير منهم يكونون عرضة لجرائم عديدة كجرائم انتهاك حق المؤلف وبيع أو عرض برامج حاسوب مقلدة، وجرائم النصب والاحتيال وسرقة البيانات الشخصية، وجرائم المساس بحرمة الحياة الخاصة، وكل هذا باستعمال شبكة

---

[1] جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية، المرجع السابق، ص77.

[2] الحاسوب الفائق أو الخارق أو العملاق: هو حاسوب ذو إمكانيات هائلة يستخدم لمعالجة وتخزين كما هائلا جداً من البيانات والمعلومات والبرامج، وهو لا يصلح للاستخدام الشخصي أو على مستوى مؤسسة محدودة إنما يستخدم على نطاق دولي حيث يمكنه ربط شبكة حاسبات آلية كبيرة جداً على نطاق واسع. والجدير بالذكر أن أجهزة الحاسوب العملاقة قدمت في الستينيات، وصممت في البداية من قبل "سيمور كراي"، في حين أن أجهزة الحاسوب العملاقة التي صممت في السبعينيات، كانت تستخدم عدد قليل من المعالجات فقط إلا أنه في التسعينيات، بدأت الآلات التي تحتوي على آلاف المعالجات في الظهور، وبحلول نهاية القرن العشرين، أصبحت أجهزة الحاسوب العملاقة المتوازية التي تمتلك عشرات الآلاف من المعالجات هي المعيار الأساس لهذه الأجهزة، حتى أصبح الحاسوب العملاق المسمى:(*Cray Titan*) ، هو أسرع حاسوب في العالم. كما تلعب أجهزة الحاسوب العملاقة دوراً هاماً في مجال العلوم الحاسوبية وتستخدم من أجل مجموعة واسعة من المهام المكثفة حسابياً في مختلف المجالات، بما فيها ميكانيكا الكم، التنبؤ بالطقس، أبحاث المناخ التنقيب عن النفط والغاز، المحاكاة الفيزيائية (مثل محاكاة الطائرات في أنفاق الرياح، محاكاة تفجير الأسلحة النووية وأبحاث الإدماج النووي)، أبحاث الفضاء...إلخ، أكثر تفاصيل حول الموضوع، يرجى زيارة الموقع الرسمي لموسوعة ويكيبيديا على الرابط الآتي:
https://ar.wikipedia.org/wiki/%D8%AD%D8%A7%D8%B3%D9%88%D8%A8_%D9%81%D8%A7%D8%A6%D9%82، تاريخ الاطلاع:2015/04/01 على الساعة:10:33.

الإنترنت. وخير مثال على ذلك هو قيام أشخاص مستغلين أحداث 11 سبتمبر 2001 بإنشاء مواقع على شبكة الإنترنت بغرض استقبال التبرعات للضحايا، مما جعل الحكومة الأمريكية تتدخل بتحذير رعاياها من التعامل مع هذه المواقع[1].

وفي المجال نفسه، تفطن المشرع الجزائري إلى ضرورة تجريم الاعتداءات الواقعة ضد الأشخاص باستعمال تكنولوجيا الإعلام والاتصال مثل: إساءة استخدام الحاسوب وشبكة الإنترنت والهاتف النقال، وعموما بأي وسيلة إلكترونية توفّرها التقنية الحديثة. فنصت المادتان (144) و(146) من القانون رقم: 01-09 مؤرخ في: 26 جوان2001 المعدل والمتمم لقانون العقوبات على جرائم الإهانة والسب والقذف باستعمال الوسائل الإلكترونية أو المعلوماتية، كما نصت المواد من: (303 - 303 مكرر) من (ق.ع.ج) على جرائم المساس بحرمة الحياة الخاصة للأفراد باستعمال الوسائل التقنية- و هذا ما سنتطرق اليه لاحقا بالتفصيل- . وحسنا فعل المشرع حينما قام في سياسته الجنائية الرامية لمكافحة كافة أشكال الجرائم الإلكترونية بتجريم هذه الأفعال متماشيا في ذلك مع التطورات الهائلة الحاصلة في مجال تقنية المعلومات، إذ صار هذا الفضاء الافتراضي مرتعا خصبا لأصناف كثيرة من الجرائم الإلكترونية ويمثل تحديا كبيرا للدول، مما جعلها تتكتل وتوحد جهودها لمكافحة هذا النوع من الجرائم المستحدثة.

المطلب الثالث: الطبيعة القانونية للجريمة الإلكترونية

رأينا فيما سبق أن المشرع الجزائري حاول إعطاء تعريف للجرائم الإلكترونية، فعرفها على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وعليه فهي تختلف في طبيعتها عن الجرائم التقليدية المعروفة. ولفهم هذه الطبيعة الخاصة، لا بد من التطرق أولا للطبيعة القانونية للمعلومات التي تعتبر أساس المعلوماتية، نظرا لقيمتها وطبيعتها من ناحيتي الاستئثار والانتشار في ظل تقنيات الحوسبة والاتصال(الفرع الأول)، ثم نتطرق للطبيعة الخاصة للجرائم الإلكترونية في (الفرع الثاني).

الفرع الأول: الطبيعة القانونية للمعلومات:

تحتل المعلومة في وقتنا الحاضر أهمية بالغة، فمن يمتلك المعلومة يمتلك السلطة أو القوة فأصبحت المعلومات تمثل قيمة مالية واقتصادية كبيرة، وكسلعة تباع وتشترى، وكمعطيات يمكن تبادلها باستعمال الحاسوب وشبكة الإنترنت. من جانب آخر لا يفرّق الفقه في تعريفه للمعلومات

---

[1] خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص153.

عن مصطلح البيانات، حيث تعرف المعلومات على أنها:" مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح أن تكون محلا للتبادل والاتصال أو التفسير أو التأويل أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها"[1].

وعليه يُثار التساؤل الآتي: هل المعلومة قابلة للاستئثار، ومن ثمة تكون محلا للاعتداء عليها؟ في هذا الصدد برز اتجاهان فقهيان، الأول اتجاه تقليدي يرى بأن المعلومة لا تعد قيمة في حد ذاتها بل لها طبيعة من نوع خاص، أما الثاني اتجاه حديث يرى بأن المعلومة عبارة عن مجموعة مستحدثة من القيم[2].

أولا: المعلومة لها طبيعة من نوع خاص: يرى أنصار هذا الاتجاه التقليدي أن للمعلومة طبيعة خاصة بموجبها تضفي وصف القيمة على الأشياء المادية، حيث يركز هذا المبدأ على بديهية مسلّم بها:" أن الأشياء التي توصف بالقيم، هي تلك الأشياء القابلة للاستحواذ"، ومفاد ذلك أن الأشياء التي يمكن الاستئثار بها هي التي تكون لها قيم، وبالتالي فمن غير المقبول أن تكون المعلومات قابلة للاستئثار وفق هذا الاتجاه، إلا عن طريق حق الملكية الأدبية أو الفكرية أو الصناعية[3]. وعليه فإن المعلومات المختزنة التي لا تنتمي إلى المواد الأدبية أو الذهنية أو الصناعية، لا تندرج حتما في مجموعة القيم المحمية، كما لا يعني ذلك استبعاد الحماية القانونية لها، لأن الفقه والقضاء يعترفان بوجود اعتداء يعاقب عليه عند الاستيلاء على مال الغير[4]، إذن فعدم مادية المعلومة هو الذي أدى بأصحاب هذا الاتجاه استبعادها من طائفة الأموال، فوصف القيمة لا ينطبق إلّا على الأشياء المادية القابلة للاستحواذ، والمعلومات ذات طبيعة معنوية فإنها غير قابلة للاستئثار وبالتالي لا تندرج في مجموعة القيم[5].

ثانيا: المعلومات مجموعة مستحدثة من القيم: يرى أصحاب هذا الاتجاه، أن المعلومات ما هي إلا مجموعة من القيم المستحدثة، حيث يرى الأستاذ: كاتالا *(Catala)*"أن المعلومة المستقلة عن دعامتها المادية تكون لها قيمة قابلة للاستحواذ، وذلك لأنها تقوّم وفقا لسعر السوق، متى كانت غير محظورة تجاريا، كما وأنها منتج بصرف النظر عن دعامتها المادية وعن عمل من قدمها، كما أنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه". وبذلك أضفى

---

[1] سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية-دراسة تحليلية، دار الكتب القانونية، دار شتات للنشر والبرمجيات مصر،2011، ص33.

[2] محمد سامي الشوا، المرجع السابق، ص178.

[3] أحمد خليفة الملط، المرجع السابق، ص104.

[4] سامي جلال فقي حسين، التفتيش، المرجع السابق، ص ص44-45.

[5] طارق إبراهيم الدسوقي عطية، المرجع السابق، ص263.

وصف القيمة على المعلومة بناء أولا على قيمتها الاقتصادية، وثانيا علاقة التبني التي تجمع بينها وبين مؤلفها مما يقودنا إلى الإقرار بوصفها قيمة مستحدثة[1].

من جانب آخر، تعتبر المادة في العلوم الطبيعية كل ما يشغل حيّزا ماديا في فراغ معين يمكن قياسه، وبالتالي فبرامج الحاسوب تشغل حيزا ماديا يمكن قياسه بوحدات مثل: (البايت والكيلوبايت والميجابايت والجيجابايت...إلخ)، رغم أن هذه البيانات تأخذ شكل نبضات إلكترونية تمثل الرقمين(0-1)، فهي تشبه التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبل الأشياء المادية[2]، وهو نفسه ما ذهب إليه المشرع الجزائري حينما اعتبر الكهرباء شيء ملموس يمكن أن يكون محلا للسرقة، وذلك بموجب نص المادة (2/350) من قانون العقوبات"...وتطبق نفس العقوبات على اختلاس المياه والغاز والكهرباء...".

وعليه تعتبر المعلومات هي جوهر المعلوماتية، وهي مجموعة مستحدثة من القيم تأخذ فيها بيانات ومعطيات الحاسب الآلي وصف المال[3]، لذا أحاطها المشرع بحماية قانونية من شتى أنواع الاعتداءات عليها، بقصد الاستخدام الأمثل لها في تخصصات ومجالات كثيرة كالأمن والدفاع والبحوث العلمية، والتعامل مع قواعد البيانات والأنظمة المعلوماتية التي تتيح المعالجة الآلية للمعطيات ومختلف شبكات الاتصال.

من جهة أخرى، وبالرجوع إلى تعريف البرنامج المعلوماتي على أنه :" سلسلة من التعليمات المحررة بلغة خاصة، والمستعملة من طرف الحاسوب من أجل تنفيذ عملية محددة" [4]، قام المشرع الجزائري بإضفاء الحماية القانونية على مصنفات الإعلام الآلي المتمثلة أساسا في برمجيات الحاسوب وقواعد البيانات، وذلك من خلال الأمر رقم: 03-05 المؤرخ في: 19 يوليو 2003 المتعلق بحقوق المؤلف والحقوق المجاورة[5]، حيث نصت المادة (04/أ) على اعتبار برامج الحاسوب من بين المصنفات الأدبية المحمية. وبالتالي اتجه المشرع الجزائري إلى اضفاء الحماية القانونية على المكونات المعنوية للحاسوب باعتبارها قيم مستحدثة، والمتمثلة في البرامج وقواعد البيانات وأنظمة

---

[1] أحمد خليفة الملط، المرجع السابق، ص ص107-108.

[2] سامي جلال فقي حسين، التفتيش، المرجع السابق، ص46، راجع أيضا، طارق إبراهيم الدسوقي عطية، المرجع السابق، ص264.

[3] محمود أحمد عبابنة، المرجع السابق، ص21.

[4] عبد الهادي بن زيطة، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية، الجزائر، ط1، 2007 ، ص12 ، راجع أيضا بشرى النية، المقال السابق، ص ص45-48.

[5] الأمر رقم:03-05 المؤرخ في:19 يوليو سنة 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، (ج.ر) رقم: 44 المؤرخة في:23 يوليو سنة 2003، ص ص3-22 .

المعالجة الآلية للمعطيات، وذلك من خلال تعديل قانون العقوبات وقانون الإجراءات الجزائية وبموجب نصوص خاصة كما سنرى لاحقا.

الفرع الثاني: الطبيعة الخاصة للجرائم الإلكترونية:

تعد الجرائم الإلكترونية من الجرائم المستحدثة، والتي برزت نتيجة اساءة استخدام مجال تكنولوجيات الإعلام والاتصال، غير أن مكافحة هذا النوع من الجرائم يلقى صعوبات جمّة نتيجة الطبيعة الخاصة لها، ويرجع السبب في ذلك، كون المعلومات هي محور ارتكاز هذا النمط من الجرائم، ففي هذا المجال تقول الدكتورة (هدى قشقوش) في محاولتها تحديد الطبيعة القانونية الخاصة للجرائم الالكترونية:" يجب أن نعترف بأننا بصدد ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، ففي معظم حالات ارتكاب الجريمة، ندخل في مجال المعالجة الإلكترونية للبيانات"[1]، كما تشير أيضا إلى أن تحديد هذه الطبيعة يستلزم "إضافة مجال معالجة الكلمات أو معالجة النصوص، إذ هي عملية وثيقة الصلة بارتكاب الجرائم، وأن القانون الجنائي عاجز عن مواجهة هذا التطور المعلوماتي لعجز نصوصه، وللتطور السريع في مجال المعلوماتية"[2].

من جانب آخر تتخذ هذه الجرائم طبيعة خاصة من حيث تكييفها القانوني، إذ لم تكن النصوص التقليدية مخصصة لهذا النوع المستحدث من الجرائم، وتطبيقها أدى إلى سلسلة من المشكلات كاعتبار المعلومات مالا يمكن الاعتداء عليه، أو ما تعلق بمسألة الاثبات كالحصول على دليل مادي، لأن المجرم الإلكتروني يقوم بكل بساطة بمحو أدلة الإدانة في لحظات، كما تظهر الصعوبة أيضا في حالة إجراء التفتيش الواقع على المكونات المعنوية للحاسوب، أو في حالة اعتراض المراسلات، فقد تكون البيانات المبحوث عنها مشفّرة مما يُثير مسألة مدى مشروعية إجبار الجاني على فك الشيفرة الخاصة به[3]، إضافة إلى صعوبة ملاحقة مرتكبي الجرائم الإلكترونية الذين يقيمون في دولة أجنبية لا تربطها اتفاقية بالدولة التي تحقق فيها السلوك الإجرامي أو جزء منه، على اعتبار أن هذه الجرائم، هي جرائم عابرة للحدود بسبب ما توفره شبكة الإنترنت من حرية الإبحار في هذا العالم الافتراضي دون قيود أو حدود[4] .

---

[1] هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، مصر ،1992، ص5 وما بعدها.

[2] المرجع نفسه، ص 5 وما بعدها.

[3] محمد علي سالم وحسون عبيد هجيج، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، كلية القانون، جامعة بابل، العراق المجلد14، العدد6، 2007، ص91.

[4] المقال نفسه، ص91-92.

على ضوء الاعتبارات السابقة، يمكن القول بأن الجرائم الإلكترونية لها طبيعة خاصة، فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود[1]سواء ما تعلق بالجانب الموضوعي كتحديد أركان الجريمة بدقة واستحداث نصوص خاصة بها تتماشى وهذه الطبيعة، أو ما تعلق بإجراءات ملاحقة مرتكبيها لأنها تتم في بيئة افتراضية يصعب معها تطبيق الإجراءات التقليدية كالتفتيش والحجز مثلا، وهذا ما عمل عليه المشرع الجزائري بمراعاته لهذه الطبيعة الخاصة أثناء سنّه للنصوص القانونية المتعلقة بمكافحتها.

المطلب الرابع: خصائص الجرائم الإلكترونية وكيفية ارتكابها

نظرا للطبيعة المستحدثة للجرائم الإلكترونية فهي تنفرد بخصائص تميّزها عن غيرها من الجرائم سواء بالنسبة للجريمة أو بالنسبة للمجرم الإلكتروني، وهي في تصاعد مستمر نظرا لإساءة استخدام تقنية المعلومات والفرص التي توفرها مثل: عدم إمكانية التعرف على شخصية المجرم الإلكتروني وقرصنة الأنظمة المعلوماتية وسرقة الهُويات ونشر الإباحية...إلخ[2] (الفرع الأول). ومع تسارع وتيرة الاعتماد على الحواسيب في عالم المصارف والأموال وإدارة المشروعات وسائر ميادين الأعمال وتعاظم دورها في تسيير شؤون المجتمعات في شتى ميادين الحياة، أصبحت هدفا بالغ الأهمية للمجرمين الإلكترونيين الذين يرتكبون جرائمهم عبر مراحل، كما يستخدمون أساليب وأدوات تقنية يصعب معها كشفهم وملاحقتهم (الفرع الثاني).

الفرع الأول: خصائص الجريمة الإلكترونية والمجرم المعلوماتي:

تتميز الجرائم الإلكترونية المرتكبة بواسطة الكمبيوتر سواء كأداة للجريمة أو كهدف لها بخصائص متفردة عن باقي الجرائم، نظرا لطبيعتها الخاصة فهي تتم في وسط افتراضي يخلق صعوبات بالغة سواء في مجال اكتشافها أو في مجال ملاحقة مرتكبيها، بما يترك فرصا لإفلات المجرم من العقاب. كما ينسحب هذا أيضا على المجرم الإلكتروني الذي تتوفر فيه مميزات ينفرد بها على باقي المجرمين التقليديين.

أولا: خصائص الجرائم الإلكترونية: يمكن تلخيص أهمها كما يأتي:

أ- **جرائم عابرة للحدود:** إن ربط العالم بشبكات اتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت، مكّن من انتشار الثقافة وتبادل المعلومات والتقارب بين الشعوب، ولكن

---

[1] يوسف المصري، المرجع السابق، ص217.

[2] *Myriam Quéméner et Yves Charpenel,Op.Cit,p.13.*

للأسف أدي أيضا إلى عولمة الجريمة ومنها الجرائم الإلكترونية، فهي لا تعترف بالحدود الإقليمية للدول ولا بالمكان ولا بالزمان، وأصبحت ساحتها العالم أجمع. ففي مجتمع المعلومات تذوب الحدود الجغرافية بين الدول، لارتباط العالم بشبكة واحدة، حيث إن أغلب الجرائم المرتكبة عبر شبكة الإنترنت، يكون الجاني فيها في دولة ما والمجني عليه في دولة أخرى في وقت يسير جدا، متسببة في أفدح الخسائر خاصة مع تعاظم دور شبكة الإنترنت، والذي أعطى بعدا آخرا خاصة في مجال التجارة الإلكترونية[1]، حيث يفصل بين الدول آلاف الأميال مما خلف مشكلات قانونية عديدة كتحديد الدولة صاحبة الاختصاص القضائي، وكذا القانون الواجب التطبيق، إضافة إلى الإشكالات المتعلقة بإجراءات الملاحقة القضائية وصعوبة التعاون القضائي بين الدول نظرا لطبيعة هذه الجرائم[2].

ونتيجة للخسائر الكبيرة التي تتسبب فيها هذه الجرائم، تعالت الأصوات الداعية إلى التعاون الدولي المكثف للتصدي لها عن طريق إبرام الاتفاقيات والمعاهدات وتسهيل إجراءات التعاون والمساعدة القضائية بين الدول، فقد تتأثر دول عدة بجريمة إلكترونية واحدة تخلق مشكلات كثيرة مثل: تحديد الدولة صاحبة الاختصاص القضائي وحول القانون واجب التطبيق وإجراءات الملاحقة القضائية، فعولمة الجريمة المنظمة[3] تقتضي عولمة مكافحتها أيضا بواسطة التعاون الدولي في صوره المتعددة.

في هذا الشأن سارع المشرع الجزائري إلى التصديق على نصوص الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية[4]، حيث نصت في مادتها الأولى :" تهدف هذه الاتفاقية إلى تعزيز التعاون العربي لمنع ومكافحة الجرائم المنظمة عبر الحدود الوطنية"، كما نصت بموجب المادة (21) منها على تجريم ارتكاب أو المشاركة في ارتكاب الأفعال التي تقوم بها

---

[1] محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية–دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة باجي مختار عنابة، الجزائر، 2011، ص28.

[2] نهلا عبد القادر المومني، المرجع السابق، ص51.

[3] يقصد بالجريمة المنظمة: مشروع إجرامي له نوع من الديمومة يمارس عدة أنشطة إجرامية ، ويقوم عليه عدد من الأشخاص متفقون أو متعاونون على استثمار المخطط والحصول على الربح من خلال السوق غير المشروعة، يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، منشورات مركز كردستان للدراسات الاستراتيجية، السليمانية، مصر، 2007، ص72.

[4] المرسوم الرئاسي رقم:14–251 المؤرخ في:2014/09/08، يتضمن التصديق على الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المحررة بالقاهرة بتاريخ:2010/12/21، (ج. ر) رقم:56 المؤرخة في:2014/09/25، ص ص4–15.

جماعة إجرامية منظمة في نطاق الاستعمال غير المشروع لتقنية أنظمة المعلومات[1]، وتدخل مكافحة الجرائم الإلكترونية ضمن هذا الإطار لأنها تتميز بأنها جرائم عابرة للحدود. وفي السياق نفسه قام المشرع أيضا بالتصديق على (إ.ع.م.ج.ت.م)، والتي تنص في مادتها الأولى على:" تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها"، والتي ستشكل إضافة جديدة في مجال مكافحة الجرائم الإلكترونية في الجزائر.

ب- جرائم يصعب اكتشافها: يمكن رد الأسباب التي تقف وراء صعوبة اكتشاف الجرائم المعلوماتية إلى عدم تركها لآثار خارجية كما في الجرائم التقليدية، فهي تتم في بيئة افتراضية *(Virtual Environment)*، ناهيك على أن الجاني يمكنه ارتكاب الجريمة في دولة أو قارة أخرى كما توفر التقنية المعلوماتية للمجرم إخفاء آثار الجريمة عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية وبالتالي محو آثاره، مما يخلق صعوبات بالغة لسلطات البحث والتحري في ملاحقته وضمان عدم إفلاته من العقاب، خاصة أن تنفيذها لا يتطلب وجود الفاعل في مكان الجريمة، بل يمكنه تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل سواء كان من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة ...إلخ.

للأسف يلعب المجنى عليه في الجرائم الإلكترونية دورا سلبيا في الكشف عنها، فمن جهة يمتنع في الغالب عن التبليغ عنها لسببين الأول صعوبة تحديد هوية المجرم الإلكتروني، وثانيا التحديات التقنية لاستخلاص الدليل الإلكتروني[2]، ناهيك عن اعتبارات أخرى قد تكون شخصية أو مالية أو متعلقة بالسمعة. وقد يسعى إلى التعتيم علي المحققين وتضليلهم حتى لا يكتشفوها، لهذا لا نعجب إذا وجدنا أن أكثر تلك الجرائم لم تكتشف إلا بمحض الصدفة، وهناك من يشير إلى أن هذه الجرائم لم يكتشف منها إلا ما نسبته 01 % فقط، وما تم الإبلاغ عنه إلى السلطات المختصة لم يتعد 15 % من النسبة السابقة، وحتى ما طرح أمام القضاء من هذه الجرائم فان أدلة الإدانة فيه لم تكن كافية إلا

---

[1] تنص المادة (21) من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية على:" تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي لتجريم ارتكاب أو المشاركة في ارتكاب الأفعال الآتية التي تقوم بها جماعة إجرامية منظمة في نطاق الاستعمال غير المشروع لتقنية أنظمة المعلومات :

- الاختراق غير المشروع أو تسهيل الاختراق غير المشروع على نحو كلي أو جزئي لأحد نظم المعلومات - تعطيل أو تحريف تشغيل أحد نظم المعلومات - إدخال بيانات بطرق غير مشروعة في أحد نظم المعلومات أو مسح أو تعديل أو نسخ أو نشر البيانات التي يحتويها هذا النظام بطريق غير مشروع- استيراد أو حيازة أو عرض أو ترك أو إتاحة إحدى المعدات أو الأدوات أو برامج تقنية المعلومات بدون سبب مشروع بهدف ارتكاب إحدى الجرائم المنصوص عليها في الفقرات الثلاث السابقة - أي جريمة من الجرائم التقليدية ترتكب بإحدى وسائل تقنية أنظمة المعلومات".

[2] *CHRISTIANE FERAL-SCHUHL, Le Droit à L'épreuve, Quatrième édition, Op.Cit,p.651.*

في حدود الخمس 5/1[1]. ومن جهة أخرى، تحرص الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو القرصنة أو لخسائر مادية فادحة عدم الكشف عن ذلك حتى لموظفيها، وتكتفي باتخاذ إجراءات داخلية دون إبلاغ السلطات القضائية المختصة، وهذا تجنبا للإضرار بسمعتها واهتزاز الثقة فيها[2].

وعموما هناك عدة أسباب تحول دون اكتشاف الجرائم الإلكترونية منها:

- التكنولوجيا المعقدة وقدرة التخزين الهائلة والسرعة البالغة التي يعمل بها الحاسوب.
- عدم وجود خطط بديلة لدى ضحايا الجرائم الإلكترونية للرد عليها وتفادى أضرارها[3].

ج- جرائم ناعمة: تختلف الجرائم المعلوماتية عن الجرائم التقليدية التي تتطلب أحيانا استخدام العنف، كما في جرائم القتل والضرب والجرح والسرقة وجرائم الإرهاب...إلخ، إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفا، بل تتطلب مواصفات خاصة كالذكاء وامتلاك الوسائل المناسبة وقدرة على التعامل مع شبكة الإنترنت. فنقل بيانات من كمبيوتر إلى أخر أو المساس بأنظمة المعالجة الآلية للمعطيات، أو الدخول غير المشروع للحاسوب أو القرصنة والسطو الإلكتروني على الأرصدة وبيانات بطاقات الائتمان، لا يتطلب أي عنف سواء مادي أو معنوي ولا يبذل فيه الجاني أي جهد عضلي، فهي جرائم هادئة بطبيعتها[4]. فلا يحتاج المجرم الإلكتروني إلى العنف، وإنما يحتاج إلى مهارة وفن ودقة في استعمال تقنية المعلومات مثل: استخدام ما يعرف بالقنابل المنطقية والفيروسات المعلوماتية...إلخ، كما أن معظم هؤلاء من الشباب المثقفين ذوي الاختصاصات العالية في مجال الحاسوب مما يخلق صعوبات إضافية لملاحقتهم[5].

د- جرائم يصعب اثباتها: إن اكتشاف وإثبات الجرائم المعلوماتية ليس بالأمر السهل، فهي تقع في بيئة غير تقليدية تتمثل في الحاسوب وشبكة الإنترنت، كما أن وسائل المعاينة التقليدية لا تفلح غالبا في إثبات هذه الجرائم نظرا لطبيعتها الخاصة، حيث تكون البيانات عبارة عن نبضات وذبذبات إلكترونية تنساب عبر الأثير، وبالتالي فالنشاط الإجرامي هنا يكون غير محسوس وباستطاعة المجرم الإلكتروني، اختراق كمبيوتر المجنى عليه فيدمر نظامه أو المعطيات المخزنة فيه أو يتلاعب بها أو

---

[1] محمد خليفة، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 01، 2009، ص26.

[2] حنان ريحان مبارك المضحكي، المرجع السابق، ص39.

[3] عمر محمد أبو بكر بن يونس، التحكم في جرائم الحاسوب وردعها(المراقبة الدولية للسياسة الجنائية –ملخص الترجمة العربية لمرشد الأمم المتحدة لعام1999)، دار النهضة العربية، مصر، ط1، 2005، ص28.

[4] نهلا عبد القادر المومني، المرجع السابق، ص 58.

[5] نعيم مغبغب، حماية برامج الكمبيوتر، منشورات الحلبي الحقوقية، لبنان، ط2، 2009 ، ص141.

يطلع على مضمونها[1]. من جهة أخرى قد تؤثر مشكلات استخلاص الدليل الرقمي لإثبات الجريمة الإلكترونية على مبدأ الاقتناع الشخصي للقاضي الجزائي، وبالتالي عدم الأخذ به مما يسمح بإفلات المجرم من العقاب[2]، حيث يستطيع المجرم المعلوماتي التخلص من الآثار المادية لجريمته بفضل التقنية المعلوماتية، التي تسمح له بامتلاك الوقت الكافي لتغيير أو تدمير الأدلة التي تثبت تورطه دون أن يتم التعرف عليه، وفي وقت لا يكاد يذكر يحتسب بالثواني[3].

من جانب آخر، تبرز مشكلة نقص الخبرات اللازمة لأعضاء الجهاز القضائي المكلف بالبحث والتحري عن هذا النوع من الجرائم بسبب طبيعتها الخاصة وخصائصها المتفردة، ونوعية الجناة، لذا لا بد من العمل وبصفة دورية على تكوينهم وتدريبهم على استعمال التقنيات المتقدمة في مجال المعلوماتية خاصة وأنها تتطور بصورة مذهلة.

لم يقف الأمر عند هذه الخصائص المميزة للجريمة الإلكترونية، بل تعداه إلى انفراد المجرم الإلكتروني أيضا بخصائص تميزه عن غيره من المجرمين التقليديين، فما هي يا ترى؟.

ثانيا: خصائص المجرم المعلوماتي: بالرجوع إلى تعريف للجريمة الإلكترونية بدلالة مرتكبها فهي: "قيام شخص ما مكّنته معرفته واستخدامه لأجهزة الحاسوب والإنترنت، أو معرفته لأحدهما من ارتكاب الجريمة المختارة"[4]، وانطلاقا من تفرد الجرائم الإلكترونية بخصائص عديدة، ينسحب ذلك أيضا على المجرم المعلوماتي الذي تتوفر فيد مميزات كالتخصص والاحترافية، إضافة إلى الذكاء وعدم استعمال العنف.

أ- التخصص والاحترافية:

1- التخصص: رأينا سلفا أن ارتباط الجرائم المعلوماتية بتكنولوجيا المعلومات ميّزها عن غيرها من الجرائم التقليدية، وهذا الارتباط هو نفسه من أسباب تميز المجرم المعلوماتي عن غيره من المجرمين التقليديين. لقد اتضح من مختلف الدراسات التي أجريت في هذا المجال في كل من أوروبا والولايات المتحدة الأمريكية، أن أغلب مرتكبي هذه الجرائم هم من الشباب الذين تتراوح أعمارهم بين 25 و45 سنة معظمهم من ذوي الاختصاص العالي، مما جعل البعض يشبههم بالمجرمين ذوي "الياقات البيضاء"[5]، وأنهم يتسمون بالحرص الشديد خشية ضبطهم وافتضاح أمرهم[6].

---

[1] محمد حماد مرهج الهيتي، الجريمة المعلوماتية- دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني، دار الكتب القانونية، مصر -الإمارات، 2014، ص95.

[2] *André Lucas et Autres, Op.Cit,pp.590-591.*

[3] محمد حماد مرهج الهيتي، الجريمة المعلوماتية، المرجع السابق، ص96.

[4] عادل عزام سقف الحيط، المرجع السابق، ص194.

[5] محمد سامي الشوا، المرجع السابق، ص5.

[6] حسين الغافري، ومحمد الألفي، جرائم الإنترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة، مصر، 2008، ص41.

كما تبين في كثير من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يعكس أن المجرم الذي يرتكب الإجرام المعلوماتي هو مجرم في الغالب متخصص، فهو يمتلك معارف في مجال تكنولوجيا المعلومات إضافة الى إدراكه بظروف ومحيط الجريمة[1]. تجدر الإشارة إلى أن توفر البراعة والمهارة في استعمال الحاسوب ليس حكرا على أصحاب التخصص في هذا المجال، وباعتبار أن المعلوماتية صارت متاحة للجميع نتيجة انتشار الحواسيب وشبكة الإنترنت وثقافة استعمالهما، إذ يمكن لكل من يمتلك القدرة على التعامل مع الحاسوب ويتتبع التقنيات الجديدة في مجال المعلوماتية، أن يكتسب مهارة كبيرة وبالتالي ارتكاب جرائم في هذا المجال.

2-الاحترافية: يتمتع المجرم المعلوماتي باحترافية كبيرة في تنفيذ جرائمه، حيث يرتكبها بواسطة الكمبيوتر الأمر الذي يقتضي الخبرة والإدراك الواسعين والمهارة التقنية اللازمة لتحقيق أهدافه الإجرامية. إن المقصود بالمهارة في هذا المجال أن يكون المجرم على درجة من العلم والدراية في التعامل في مجال المعالجة الآلية للمعطيات، والتي قد يكتسبها من خلال الدراسة المتخصصة أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات[2]، كاختراق نظم الكمبيوتر العائدة للشركات الصناعية والتجارية والقيام بعمليات الاحتيال والتزوير عن طريق شبكة الإنترنت بقصد تحقيق مكاسب مادية أو غيرها[3]. كما تمكّنهم احترافيتهم من التغلب على العقبات التي أوجدها المتخصصون في مجال البرمجيات لتوفير أنظمة لحماية الكمبيوتر من كافة أشكال القرصنة[4] كما في حالة البنوك والشركات والمؤسسات الصناعية والعسكرية...إلخ[5].

---

[1] فريد منعم جبور، حماية المستهلك عبر الإنترنت ومكافحة الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2010 ص189.

[2] رشيدة بوكر، المرجع السابق، ص94.

[3] عبد الحكيم رشيد توبة، المرجع السابق، ص162.

[4] ومن قضايا القرصنة الشهيرة:

- قرصنة شبكة حاسوب قصر الإليزيه في شهر مارس 2012، من طرف هاكرز أمريكي، حيث تم الدخول إلى الكمبيوتر الشخصي للرئيس الفرنسي نيكولا ساركوزي *(Nicolas Sarkozy)* والحصول على معلومات سرية للغاية.
- قرصنة وكالة الفضاء الأمريكية *(NASA)* في شهر فيفري 2012 من طرف هاكرز روماني ، أين تم كشف ثغرات عديدة في نظام الأمن الخاص بالوكالة والبنتاجون *(pentagone)*، إضافة إلى نشر معلومات سرية وفيديو يُظهر قرصنته للوكالات الأمريكية.
- قرصنة شركة سوني *(Sony)* في شهر ماي 2011 ، أين تم اختراق 130 خادم *(Serveurs)* يخزنون قرابة 77 مليون حساب *(PSN)*، مما عرّض الشركة إلى خسائر كبيرة، راجع، *Redouane Semlali, art-Cit,p.40*

[5] حسين الغافري، ومحمد الألفي، المرجع السابق، ص41.

ونظرا للعوائد المالية الكبيرة للجرائم الإلكترونية، يعود كثير من مجرمي المعلوماتية إلى ارتكاب جرائم أخرى في مجال الكمبيوتر، انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم إلى المحاكمة في المرة الأولى، مما يجبرهم على العودة إلى الإجرام، وتفادي الأخطاء السابقة، وقد ينتهي بهم الأمر الى تقديمهم إلى المحاكمة مرة أخرى.

ب- الذكاء وعدم استعمال العنف:

1- الذكاء: المجرم المعلوماتي ليس شخصية عادية، فهو يتصف بالذكاء، وهو على قدر كبير من سرعة الفهم وسعة الاطلاع والنشاط الذهني المتقدم الذي يسعى إلى خداع الكمبيوتر، إضافة الى القدرة على التعامل مع كل ما يصدر في مجال استعمال الكمبيوتر وبرامجه، واستغلال شبكة الإنترنت، فيستطيع التلاعب بالمعلومات أو الكيانات المنطقية للحاسوب كزرع فيروسات لنسخ البيانات أو تدميرها...إلخ[1].

2- عدم استعمال العنف: بمعنى أن المجرم لا يلجأ للمجهود العضلي كما في الجرائم التقليدية فالجرائم المعلوماتية هي جرائم هادئة بطبيعتها *(Soft Crimes)* لا تحتاج للعنف[2]، فهذه الجرائم تنتمي إلى إجرام الحيلة، أو ما يعرف بجرائم "الياقة البيضاء"، كما يتمتع فيها المجرم بالتكيف الاجتماعي، أي لا يناصب أحد العداء كما أنه على درجة عالية من الثقافة.

بعد تعرفنا على خصائص الجريمة الإلكترونية والمجرم المعلوماتي، ما هي مراحل ارتكابها والأساليب المستخدمة في ذلك؟

الفرع الثاني: مراحل الجريمة الإلكترونية وأساليب ارتكابها:

تمر الجريمة الالكترونية بمراحل عديدة لارتكابها، كما تتنوع الأساليب والأدوات التي يستخدمها المجرم بقصد الإفلات من العقاب.

أولا: مراحل ارتكاب الجريمة الالكترونية: يمكن ارتكاب الجرائم الإلكترونية في أي مرحلة من المراحل الأساسية لتشغيل نظام الحاسوب، لكي نفهم هذه المراحل لا بد من التطرق أولا للمقصود بنظام التشغيل وكيفية عمله، ثم نتناول بعد ذلك المراحل التقنية لارتكاب الجريمة.

1- مفهوم نظام التشغيل وكيفية عمله: لا يمكننا فهم مراحل الجريمة الإلكترونية دون التعرف على نظام تشغيل الحاسوب وكيفية عمله، فكما رأينا سلفا، يتكون الحاسوب من مكونات مادية *(Hardware)* ومكونات منطقية *(Software)*، حيث تمثل المكونات المادية جسد الحاسوب أي: الأجهزة الملموسة كالشاشة، ولوحة المفاتيح، والمعالج، والذاكرة...إلخ، بينما تمثل المكونات المنطقية

---

[1] يوسف أبو الحجاج، المرجع السابق، ص20.

[2] نهلا عبد القادر المومني، المرجع السابق، ص ص 57-58.

أو البرمجية روح الحاسوب، وهي التي تتحكم في المكونات المادية وتوجه عملها، وليس من السهل استخدام المكونات المادية للحاسوب دون برامج، فالحاسوب دون برامج كالجسد بلا روح أو كالسيارة بلا وقود. إن أهم جزء في هذه البرامج والذي تعتمد عليه البقية في عملها هو نظام التشغيل *(Operating System)*، هناك عدة تعريفات له منها أنه:" مجموعة من البرمجيات المتكاملة فيما بينها لتوجيه أجهزة الحاسوب للعمل به، بحيث يستدعي برامج المساعدة وبرامج التطبيقات من وحدات التخزين إلى الذاكرة"[1]، وفي تعريف آخر:" نظام التشغيل هو ذلك البرنامج الذي يثبت على الحاسوب ليدير جميع موارده ويتيح للمستخدم واجهة *(User Interface)* تمكنه من التعامل مع المكونات المادية بكل سهولة ويسر"[2]. من أشهر نظم التشغيل: نظام *(DOS)*، ونظام أونيكس*(UNIX)* ونظام النوافذ *(WINDOWS)*.

ويمكن القول أن نظام التشغيل، هو جسر لتنفيذ برامج المستخدم، حيث يقوم بالمهام الأساسية مثل [3]:

- تنفيذ تطبيقات المستخدم (الإدخال– المعالجة– الإخراج).
- توفير بيئة مناسبة وملائمة للاستخدام.
- الاستفادة القصوى من الموارد، وذلك بجعلها تعمل بشكل فعّال.
- تخصيص مصادر الحاسوب (الذاكرة، القرص الصلب، الوصول للأجهزة الملحقة...إلخ).
- ترتيب أولوية التعامل مع الأوامر.
- التحكم في أجهزة الإدخال والإخراج مثل لوحة المفاتيح، وتسهيل التعامل مع الشبكات وإدارة الملفات...إلخ.

وعلى هذا الأساس، هنالك الكثير من نظم التشغيل المعاصرة، تختلف باختلاف الأنظمة والأجهزة والأغراض، فمنها ما يستخدم لإدارة جهاز واحد شخصي ومنها ما يستخدم لإدارة أجهزة متعددة المعالجات...إلخ، ومن نظم التشغيل الشهيرة المستخدمة حاليا نذكر ما يأتي[4]:

أ– **ميكروسوفت ويندوز *(Microsoft Windows)*** : وهي من أنظمة التشغيل الشهيرة تستخدمها نسبة عالية من الحواسيب، والتي تعمل على معالجات أنتل*(Intel)* والمعالجات المتوافقة معها، توجد منها عدة نسخ مثل:*(Windows xp..Windows7...)*.

1 بشرى النية، المقال السابق، ص40.

2 عبد الرحمان أحمد محمد عثمان، مفاهيم نظم التشغيل، (ب. د. ن)، ط2، 2013، ص18.

3 المرجع نفسه، ص18.

4 المرجع نفسه، ص ص25–26.

ب- يونيكس *(Unix)* :صمّم في عام 1974 من طرف العالمين: دينيس ريتشي *(Dennis Ritchie)* وكان طومسون *(Ken Thompson)*، بينما كانا يعملان في معامل *(AT & T Bell)* كان الهدف منه وضع نظام تشغيل صغير ومتنقل. ثم انتشر في الجامعات ومراكز البحوث في عام 1991 ، ومن نسخ يونيكس المشهورة *(V Unix)* و*(BSD)*، وهو أول نظام تشغيل يكتب بالكامل بلغة برمجة عالية.

ت- ماكنتوش *(MAC)* : صُمم ليعمل على أجهزة أبل *(Apple)*ماكنتوش التي تنتشر في دور الطباعة والنشر، وهو قوي وسهل الاستخدام وقد أخذت ويندوز فكرة النوافذ وسطح المكتب من هذا النظام حيث كان أول نظم تشغيل يدعم الواجهات الرسومية والأيقونات والقوائم على سطح مكتب.

ت- توزيعات لينكس *(Linux)* : هي نسخة مصغرة من يونيكس صمّمت لتعمل على الحاسبات الشخصية، وهو مفتوح المصدر حيث يتيح حرية تعديل الشفرة وإعادة التوزيع، ويوجد منها مئات التوزيعات أحدثها وأشهرها توزيعه (أوبونتو) التي تدعم كل لغات العالم واجهة وكتابة بما فيها اللغة العربية.

2- المراحل التقنية لارتكاب الجريمة الإلكترونية: بعد التعرف على كيفية عمل نظام تشغيل الحاسوب، وأنه لا غنى عنه للمجرم الإلكتروني لارتكاب جريمته، إذ يتم تشغيل نظام المعالجة الآلية للبيانات داخل الحاسوب وفق ثلاثة مراحل هي مرحلة الإدخال ومرحلة المعالجة ومرحلة الإخراج، إذ يتطلب إنجاز كل مرحلة من هذه المراحل نوعية خاصة من البرامج والتطبيقات، ومع ذلك لا يمكن بالنظر لطبيعة هذه الجرائم إلا ارتكابها في وقت محدد يعتبر هو الأمثل بالنسبة لمراحل التشغيل[1] وعموما يتم ارتكاب هذه الجرائم وفق المراحل الآتية:

أ- مرحلة الإدخال *(Input Data)*: في هذه المرحلة يتم إدخال البيانات التي تترجم إلى لغة تفهمها الآلة، بحيث يسهل التلاعب فيها، ومثال ذلك قيام المجرم الإلكتروني بتغيير أو تزوير البيانات عن طريق التسلل الإلكتروني للمعطيات في فاتورة الهاتف مثلا قبل طبعها في شكلها النهائي وإرسالها للزبون، بحيث يتمكن من حذف بعض المكالمات، أو قيام أحد الطلبة بتغيير نقاطه المسجلة في النظام قصد الحصول على معدل يمكنه من النجاح[2]، وهذه المرحلة هي التي يتم فيها ارتكاب الجانب الأكبر من الجرائم الإلكترونية[3]. وادراكا من المشرع الجزائري بخطورة هذه المرحلة، نص على تجريم إدخال المعطيات بطريق الغش أو إزالتها أو تعديلها بموجب نص المادة(394 مكرر 1)

---

[1] أحمد خليفة الملط، المرجع السابق، ص92.

[2] عماد مجدي عبد الملك، المرجع السابق، ص46.

[3] أحمد خليفة الملط، المرجع السابق، ص92.

من قانون العقوبات التي تنص على: " يعاقب بالحبس من ستة أشهر(6) إلى ثلاث (3) سنوات وبغرامة من 500.000 الى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

ب-مرحلة المعالجة *(Data Processing):* في هذه المرحلة يمكن للمجرم الإلكتروني إدخال تعديلات على البرامج الجاهزة *(Soft Ware)*، والتي تقوم بتشغيل البيانات للوصول إلى نتائج محددة، فعن طريق التلاعب في النظام المعلوماتي، يتم دس تعليمات غير مصرح بها، أو تشغيل برامج جديدة تلغي جزئيا أو كليا عمل البرامج الأصلية[1]، ومثال ذلك استخدام برنامج معين لتقريب الأرقام المتعلقة بالعمولات البنكية على حساب أحد الزبائن، أو تجميع الفروق بين الأرقام المقربة والأرقام الفعلية وإضافتها إلى حساب سري آخر للزبون نفسه، تبدو هذه الفروق بسيطة ولكنها ستكون ضخمة إذا تمّت خلال سنوات عديدة[2].

إن الجرائم المرتكبة في هذه المرحلة تتطلب توافر معرفة تقنية ومهارات فنية خاصة لدى المجرم المعلوماتي، كأن يكون مبرمج أنظمة مثلا[3]، كما أن اكتشاف هذه الجرائم يكون صعبا للغاية نظرا لما توفره التقنية الحديثة من إمكانات هائلة في مجال تقنية المعلومات، لذا نص المشرع الجزائري في القانون رقم: 09-04 المؤرخ في 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على جملة من الإجراءات الهامة خاصة ما تعلق بإجراءات التحقيق والتفتيش وحجز المعطيات والمساعدة القضائية، والاستعانة بكل شخص له دراية وخبرة لمساعدة جهات التحقيق في الكشف عن الجرائم الإلكترونية، نظرا لطبيعتها وصعوبة التحقيق فيها، فهي تتم في بيئة افتراضية يصعب تتبع المجرم المعلوماتي، ناهيك على أن التقنية الحديثة توفر له سهولة إخفاء أثره وتدمير الأدلة، وبالتالي إفلاته من العقاب، وهذا ما سنراه لاحقا بالتفصيل.

ت- مرحلة الإخراج *(Output Data):* وهي المرحلة الأخيرة المتعلقة بالمخرجات، وتعتبر أيضا من أكثر المراحل التي ترتكب فيها الجرائم الإلكترونية، حيث تتم سرقة المعلومات أو البيانات المتعلقة بالرقابة على المخزون في إحدى المصالح مثلا، أو إنشاء بعض المعلومات الخاصة بالإجراءات الأمنية الخاضعة للفحص السري لتأمين وضع معين متعلق بسلطات عسكرية أو وزارات أو شركات أو أفراد[4]. في هذا الشأن نص المشرع الجزائري بموجب المادة (394 مكرر2) على: "

---

1 المرجع نفسه، ص92.

2 عماد مجدي عبد الملك، المرجع السابق، ص46.

3 عبد الحكيم رشيد توبة، المرجع السابق، ص171.

4 المرجع نفسه، ص171.

يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يلي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة...
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم". وبالتالي كان هدف المشرع هو عدم تمكين المجرم من استغلال هذه المخرجات سواء بالنشر أو الاستعمال أو الاتجار.

ثانيا: الأساليب المستخدمة في الجرائم الإلكترونية: توفّر التقنية المعلوماتية إمكانات هائلة في مجال استخدام الحاسوب وشبكة الإنترنت يستغلها المجرم الإلكتروني في تنفيذ جرائمه المختلفة، في هذا الشأن يستخدم المجرم أساليب كثيرة، نتناول بعضها حسب التقسيم الآتي:

1-الأساليب المستخدمة في الاعتداء على المكونات المادية للحاسوب: تتميز الجرائم الإلكترونية بأساليب متفردة يغلب عليها الطابع التقني والفني، وهذا ما يميزها عن باقي الجرائم التقليدية، فلقد استوعب المجرم الإلكتروني هذه التقنية الحديثة التي بلغت حد الخيال نظرا للإمكانات الهائلة التي توفرها كالقدرة على التخزين والمعالجة والاسترجاع والسرعة الفائقة والمرونة في التشغيل. حيث استغلوا هذه الخبرات المكتسبة في تطوير وسائل تقليدية وجديدة للاعتداء على مكونات الحاسوب سواء كانت مادية أو معنوية، ولا شك أن هذه الاعتداءات الواقعة على المكونات المادية للحاسوب تخضع في مكافحتها للمفاهيم التقليدية للجرائم المعروفة كجريمة السرقة وجريمة الإتلاف...إلخ، وعموما يمكن استخدام هذه الأساليب ذات الطابع التقليدي لارتكاب عدة جرائم يكون محلها المكونات المادية للحاسوب[1]، وتتلخص في صورتين: الأولى تتمثل في سرقة الوسائل المادية للحاسوب، والثانية في تخريبها أو إتلافها.

- **الصورة الأولى: سرقة المكونات المادية للحاسوب:** نشير إلى أنه في بداية اختراع الحواسيب لم يكن بالإمكان سرقة هذه المكونات، ويرجع السبب في ذلك إلى أنها كانت كبيرة الحجم. ونتيجة للتطورات العلمية المتلاحقة ومع انتشار الثورة المعلوماتية وظهور تقنيات مستحدثة في هذا المجال لم يبق أمر هذه المعدات كما كانت سابقا، فتقلص حجم مراكز المعالجة الإلكترونية للبيانات نتج عنه صغر حجم الحواسيب ومعداتها، ناهيك عن انتشار الحواسيب المنزلية بل تعدى ذلك إلى الحواسيب الشخصية التي صارت بحجم كف اليد، وبالتالي يمكن القول أنه مع انتشار الأنظمة الميكروية وصغر

---

[1] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشأة المعارف، الإسكندرية مصر،(ب.س.ط)، ص24.

حجمها، انتشرت معه سرقة المعدات المادية للحواسيب[1]. ومن أمثلة ذلك سرقة جهاز الحاسوب نفسه أو أحد لواحقه كالشاشة أو الطابعة أو القرص الصلب وما يحتويه من برامج ومعطيات يمكن استخدامها في عمليات الاحتيال الإلكتروني وتحويل الأموال...إلخ، أو سرقة البطاقات الممغنطة التي تستخدم لسحب النقود من الحاسوب قصد الحصول على سلع وخدمات من الشركات أو التجار[2].

ويلاحظ حاليا انتشار هذا النوع من السرقات، بل ويقع على أنظمة معلوماتية بأكملها، وغالبا ما تكون سرقة المعدات المعلوماتية ثمرة لأفعال النصب والاحتيال مثل: تمكن مواطن أمريكي من مدينة *(San Diego)* من شراء حاسوب من شركة مشهورة تدعى *(General Dynamics Corp)*، حيث قام بإعطائها عنوانا وهميا لمحل إقامته ثم اختفى[3]. وبغض النظر عن أفعال السرقة البسيطة، هناك العديد من الأساليب الأخرى المستخدمة في اختلاس المكونات المادية للحاسوب خاصة وحدة المعالجة المركزية *(CPU)*، فقد تم اختلاس قطع غيار الحاسوب يقدر ثمنها بملايين الدولارات من أحد فروع شركة *(Nixdorf)* الأمريكية، حيث عُهد لأحد مستخدميها بقطع الغيار والمكونات الإلكترونية الجديدة، ولكنه بالمقابل صنفها على أنها أشياء غير قابلة للاستعمال وألقى بها في المخلفات، ثم أعيد شراؤها مرة أخرى بثمن منخفض عن طريق شريك له يعمل تحت ستار شركة صيانة[4].

وعلى هذا الأساس، ينصح الخبراء العاملون في هذا المجال، بضرورة اتخاذ الاحتياطات المادية والفنية والأمنية من خلال اللجوء إلى الأنظمة الحديثة لحماية نظم المعلومات، سواء عن طريق المخازن المزودة بالمراقبة أو الحراسة مع ضرورة توافر أجهزة الإنذار المبكر، أو عن طريق استعمال كاميرات المراقبة...إلخ.

- **الصورة الثانية: إتلاف أو تخريب المكونات المادية للحاسوب:** تقع جريمة الاتلاف في المجال المعلوماتي على المكونات المادية المتصلة بالحاسوب وملحقاته، كالشاشة أو لوحة المفاتيح أو الفأرة أو الأشرطة أو الأقراص الممغنطة وغيرها مما لها علاقة بهذا المجال. كما أنه لا توجد أية عقبات قانونية تحول دون تطبيق النصوص التقليدية الخاصة بجريمة الإتلاف على اعتبار أن محل الجريمة مال مادي منقول مملوك للغير. ففي سنة 1983 وصف الكاتب والصحفي البريطاني *(George Orwell)* الحاسوب بأنه: "رمز لمجتمع غير إنساني أو رمز للمجتمع

---

1 محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، القاهرة، مصر، 2011 ، ص ص88-89.

2 عفيفي كامل عفيفي ، المرجع السابق، ص26.

3 محمد سامي الشوا، المرجع السابق، ص95.

4 المرجع نفسه، ص96.

الرأسمالي"، في حين وصفه بعض المجرمين في ألمانيا بأنه "الأخ الأكبر"، وعلى ضوء هذه العبارات القصيرة، نستطيع أن نحصر أساليب اتلاف أو تخريب المكونات المادية للحاسوب، والتي ترجع في الغالب إلى فعل الإنسان ذاته (كالاعتداء على الحواسيب عن طريق إتلافها أو تخريبها بإطلاق النار عليها أو إشعال النار فيها أو تفجيرها...إلخ)، أو مصادر طبيعية (كالفيضانات الزلازل...إلخ)[1].

وتبعا لذلك فإن ظاهرة الإتلاف المعلوماتي في ازدياد مستمر، وقد بدأت هذه الأفعال غير المشروعة في الولايات المتحدة الأمريكية في أوائل السبعينيات عندما قامت جماعة مناهضة لحرب فيتنام بتدمير العديد من الحاسبات الآلية، ثم انتقلت بعد ذلك إلى ألمانيا وفرنسا[2].

كما أن للتخريب المعلوماتي المنصب على المكونات المادية للحاسوب، أساليب أخرى متعددة كإدخال قطع أو أسطوانات حديدية صغيرة، أو شرائح من الألمنيوم أو قصاصات ورق في فتحات أجهزة الحاسوب لتعطيله، أو صب بعض المشروبات كالقهوة أو بعض السوائل كمحلول الملح أو سوائل التنظيف، أو قطع الكوابل والأسلاك الموصلة بالحاسوب، كما يمكن أيضا استخدام القوة المغناطيسية قصد محو محتويات الأسطوانات الممغنطة[3].

2- الأساليب المستخدمة في الاعتداء على المكونات المعنوية للحاسوب: في هذا الشأن تتنوع هذه الأساليب تبعا للتطور التكنولوجي في مجال الحوسبة والاتصال، فكلما تطورت هذه التقنيات، تطورت معها هذه الأساليب، وبصفة عامة يمكن تعريف هذه الأساليب بأنها:" برمجيات أو وسائط تقنية قابلة للتوظيف مع عتاد الحاسوب وبرمجياته لتحقيق أهداف معينة كمضايقة وإنهاك مستمر لموارد النظام المعلوماتي وتدمير قواعد البيانات، وموارد البرمجيات والنظم التطبيقية وإحداث ثغرات في النظام المعلوماتي"[4]. ومما لا شك فيه أن هناك أكثر من أسلوب أو طريقة توفرها التقنية الحديثة لارتكاب هذه الجرائم، وإن أكثر ما يتم به تنفيذ هذه الاعتداءات على المكونات المنطقية للحاسوب هي البرامج الخبيثة ذات الأثر التدميري التي تستهدف محو جزء أو كل برامج وملفات الحاسوب والبيانات المخزنة، ولكل برنامج منها تسمية شائعة تستمد عن وظائفه التدميرية[5]، لذا سنحاول التطرق إلى الأساليب الشائعة في ارتكابها وذلك كالآتي:

---

1 محمد علي العريان، المرجع السابق، ص ص 89-90.

2 المرجع نفسه، ص90.

3 هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة ، مصر، 1994، ص155.

4 حسن مظفر الرزو، المقال السابق، ص70.

5 هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص158.

●**التقاط المعلومات الموجودة بين الحاسوب والنهاية الطرفية:** تتم هذه العملية بواسطة تحويلة تعمل على تكبير الذبذبات الإلكترونية وإرسالها إلى النهاية الطرفية للقيام بعملية التجسّس[1].

●**الفاحص *(Scanner)*:** وهو عبارة عن برنامج تطبيقي أعد لأغراض الكشف الآلي عن مواطن الضعف في المضيفات المحلية والنائية *(Local et Remot Host)*،حيث تعمد هذه البرمجيات إلى قرع أبواب طرفيات *(Tcb/Ip)* والخدمات المصاحبة لها، وبذلك توفر معلومات ثمينة تعتبر موردا هاما لقراصنة المعلومات مثل: الحصول على الآلاف من كلمات السر الشخصية التي تمكنهم من الدخول غير المشروع للنظام واستغلال بياناته[2].

●**التقاط الإشعاعات الصادرة عن الجهاز المعلوماتي:** تهدف هذه العملية إلى إعادة تكوين وتغيير خصائص المعلومات، التي تبث وتنقل من خلال الأنظمة المعلوماتية، كما تحتاج هذه العملية التقنية المعقدة إلى فك شيفرة النظام[3].

●**الفيروسات:** تعتبر الفيروسات من الوسائل الأكثر استعمالا في ارتكاب الجريمة المعلوماتية من شأنها تعديل أو محو المعطيات التي يتم معالجتها آليا بما يشوه سير النظام المعلوماتي، فإذا كان بعض الفيروسات لا يتسم بالخطورة، فإن البعض الآخر منها يمكنه تخريب النظام المعلوماتي وإعاقة سيره[4]، كما تعتبر من أهم التقنيات التي تستخدم لتدمير نظم المعلومات، فيمكن تعريفها على أنها: "برنامج يصممه بعض المتخصصين بهدف تخريبي مع إعطائه القدرة على ربط نفسه ببرامج أخرى ثم يتكاثر وينتشر داخل النظام حتى يتسبب في تدميره تماما"[5]، كما يعرف الفيروس أيضا على أنه:" برنامج صغير صيغ لغرض تغيير عمل برمجيات الحاسوب دون السماح للمستخدم بمعرفة هذا الأمر"[6]. فهي تكتب بواسطة مبرمجين محترفين بغرض إلحاق الضرر بحاسب آخر، أو السيطرة عليه أو سرقة بيانات مهمة منه، وتتم كتابتها بطريقة معينة.

من جانب آخر، تصنف الفيروسات إلى تصنيفات عديدة سواء حسب مبدأ عملها أو حسب التسمية التي تتخذها، أو حسب الموقع الذي تصيبه بالتلف[7]، فهي عبارة عن برامج مشفرة مصممة بقدرة كبيرة على التكاثر والانتشار من نظام إلى آخر، ومن الفيروسات الشهيرة: فيروس(الحب) فيروس(ميليسا)، فيروس(الدودة)، فيروس (حصان طروادة)، القنبلة المعلوماتية،القنبلة المنطقية، القنبلة

---

[1] عفيفي كامل عفيفي، المرجع السابق، ص26.

[2] حسن مظفر الرزو، المقال السابق، ص 70، راجع أيضا، طارق ابراهيم الدسوقي عطية، المرجع السابق، ص527.

[3] عفيفي كامل عفيفي، المرجع السابق، ص26.

[4] *CHRISTIANE FERAL-SCHUHL, Le Droit à L'épreuve, Quatrième édition, Op.Cit,p. 601.*

[5] محمد علي العريان، المرجع السابق، ص103.

[6] حسن مظفر الرزو، المقال السابق، ص77.

[7] محمد حماد مرهج الهيتي، الجريمة المعلوماتية، المرجع السابق، ص475.

الزمنية...إلخ، ولنأخذ مثلا فيروس القنبلة الموقوتة، وهي عبارة عن برنامج مصمم بحيث تبقى ساكنة وغير فعالة وغير مكتشفة لمدة أشهر أو أعوام يحددها مؤشر زمني كتاريخ معين مثلا بحيث ينشط البرنامج عند حلوله ويؤدي مهامه الهدّامة[1].

كما تنتشر الفيروسات حينما يستقبل مستخدمي الإنترنت بواسطة البريد الإلكتروني، رسائل بريدية ملغومة بفيروسات مدمرة من مجهولين، وتنشط بمجرد فتح تلك الرسالة، وهي تعليمات غير مرخصة موضوعة في برامج بهدف إجراء عمليات غير مشروعة في وقت محدد مسبقا أو حين تتوفر شروط معينة[2]، لذلك ينصح خبراء المعلوماتية عدم فتح الرسائل الإلكترونية مجهولة المصدر، لأنها يمكن أن تشكل خطرا كبيرا على أمن المعلومات والبيانات المخزنة، ولا زالت شركات البرمجيات تعمل جاهدة على توفير برامج مضادة للفيروسات *(Antivirus)* لتوفير الحماية اللازمة لمستخدمي الحاسوب وشبكة الإنترنت. ولكن للأسف ففي كل مرة يحاول القراصنة التغلب عليها بطرح فيروسات جديدة، مما يضطر هذه الشركات إلى تحيين برامجها وإيجاد الحلول المناسبة، ويفرض عليها مزيدا من التكاليف المالية وهدرا للجهد والوقت.

●**التدخل غير المشروع في النظام المعلوماتي:** يسمح هذا الاسلوب للجاني نسخ أو تدمير البيانات، وإدخال معطيات وهمية، والتلاعب في البرامج التشغيلية وزرع الفيروسات والبرامج الوهمية ولا تتطلب العملية أكثر من جهاز حاسوب موصول بشبكة الإنترنت، مع ضرورة التعرف على كلمة السر أو شيفرة النظام[3].

●**البرامج المعدة لأغراض محددة:** تستخدم في هذه العملية برامج النظام الخاصة مثل:*(super zap)* المطور من قبل شركة *(IBM)* لاستخدامه في حالة الطوارئ قصد تجاوز قيود التحكم العادية لتنفيذ عمليات غير مشروعة[4].

●**أسلوب الباب السحري:** وهي تعليمات تعطى للحاسوب قصد السماح للمستخدم بتجاوز قيود التحكم المعتادة في النظام، وهذه التعليمات تعطى للحاسوب أثناء تطوير الأنظمة وتحذف في الغالب قبل وضع النظام أثناء مرحلة التشغيل النهائي[5].

---

[1] أمجد حسان، الفيروسات إرهابا تهدد أنظمة المعلومات، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، الجزائر، العدد 4، السداسي الأول، 2011، ص124، راجع أيضا، محمد حماد مرهج الهيتي، الجريمة المعلوماتية، المرجع السابق، ص ص476-479، وهشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص158، وأيضا، محمد أمين الرومي، المرجع السابق، ص ص26-29.

[2] عبد الحكيم رشيد توبة، المرجع السابق، ص171.

[3] عفيفي كامل عفيفي، المرجع السابق، ص26.

[4] عبد الحكيم رشيد توبة، المرجع السابق، ص171.

[5] عفيفي كامل عفيفي، المرجع السابق، ص27.

●**التزوير والخداع الإلكتروني:** يكون التزوير حينما يستخدم شخص غير مفوض رقم هوية وكلمة السر الخاصة بمستفيد مفوض للولوج إلى النظام والقيام بعمليات غير مشروعة، أما الخداع الإلكتروني فيحدث حينما يتصل آليا شخص مخادع بمستفيد مفوض ويوهمه بأنه له حق الاستفادة من خدمات النظام[1].

نستنتج في الأخير أن هذه الأساليب لا حصر لها، ومرتبطة بالتطور التكنولوجي الحاصل في مجال المعلوماتية، ولكن بالمقابل، ما هي الأدوات التي يستعملها المجرم الإلكتروني لارتكاب هذا النوع من الجرائم؟ هذا ما سنتعرف عليه فيما يأتي.

ثالثا: الأدوات المستخدمة في الجرائم الإلكترونية: رأينا سلفا أن أساليب ارتكاب الجرائم الإلكترونية لا حصر لها، فالأمر نفسه ينطبق على الأدوات المستعملة في ذلك، نتيجة التقدم الهائل الحاصل في مجال تقنية الحاسوب والاتصال. فهي من جهة توفر للمستعمل أدوات كثيرة تسهل عليه معالجة المعلومات وتخزينها واسترجاعها وإرسالها كأجهزة الحاسوب وملحقاته وبرامجه، إضافة إلى الأهمية التي تكتسيها تقنية البريد الإلكتروني الذي يمكننا من استقبال وإرسال ملفات على اختلاف أنواعها، ومن جهة أخرى تعتبر تقنية الاتصالات الحديثة والشبكات المحلية والعالمية كالهواتف النقالة والشبكة العنكبوتية...إلخ، أدوات فعّالة تمكن المجرم المعلوماتي(*Le Criminel Informatique*) من ارتكاب الجرائم الإلكترونية على اختلاف أنواعها، نتطرق إلى بعض منها فيما يأتي:

1- الحاسوب وملحقاته وبرامجه: حققت التقنيات الحديثة قفزة عملاقة في مجال صناعة الحاسوب وملحقاته، إضافة إلى التطورات الهائلة في مجال الاتصال وعلى رأسها شبكة الإنترنت حيث لم يعد من الممكن استغناء الإنسان في شتى مجالات حياته عن استعمال الحاسوب والشبكة العنكبوتية، نظرا لما توفره هذه التقنية من خدمات سريعة وغير مكلفة. لكن للأسف وككل تكنولوجيا حديثة لها سلبياتها، فقد أدى سوء استخدامها إلى اعتبار الحاسوب الأداة الأولى للجرائم الإلكترونية[2]، وذلك لسهولة استخدامه وانتشاره بين الناس، وتنوع برامجه والاحترافية التي يتعامل بها بعض الناس والتي بدأت تزداد يوما بعد يوم، فيكفي للشخص توفر جهاز حاسوب متصل بشبكة الإنترنت، إضافة إلى معرفة بسيطة بالمعلوماتية، أن يقوم بارتكاب جريمة إلكترونية ولو كانت بسيطة مثل إرسال رسالة إلكترونية بالبريد الإلكتروني تتضمن سبا أو شتما أو قذفا أو تهديدا...إلخ.

---

[1] عبد الحكيم رشيد توبة، المرجع السابق، ص172.

[2] فايز الظفيري، المقال السابق، ص492.

2- البريد الإلكتروني: وفرت لنا شبكة الإنترنت أداة بالغة الأهمية بخصوص الاستعمال الشخصي لعلبة البريد الإلكتروني، حيث عرّف جانب من الفقه البريد الإلكتروني على أنه:" طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات"[1]، فهو يستخدم كمستودع لحفظ الأوراق والمستندات الخاصة في صندوق البريد الخاص بالمستخدم، بشرط تأمينه بطرق التأمين المعروفة كالتشفير وكلمات السر *(Password)*، وغيرها من تقنيات الحماية[2]. أصبحت هذه الأداة من أسرع الوسائل التي وفرتها التقنية المعلوماتية بالمجان قصد توفير خدمات الاتصال وتبادل الملفات سواء كانت صوتية أو مرئية، فالبريد الإلكتروني أصبح بديلا عن الهواتف لأنه أداة اتصال ناجزة للمصالح خاصة في المعاملات التجارية[3]. لكنه بالمقابل يستخدمه المجرم المعلوماتي في إرسال الفيروسات على اختلاف أنواعها وأهدافها كنسخ البيانات الشخصية أو تدميرها أو تعديلها...إلخ، أو إرسال روابط لمواقع مشبوهة، كما يستخدم أيضا لترويج الشائعات والأكاذيب وغيرها، ومن الأمثلة على ذلك قضية فيروس البريد الإلكتروني الأكثر شهرة *(Melissa)* للهاكرز الأمريكي *(David Smith)*، حيث أحدث هذا الفيروس اضطرابا عالميا في خدمات البريد الإلكتروني، حيث يقوم باستنساخ نفسه ويسخّر برمجيات البريد الإلكتروني لإرسال قائمة بعناوين مواقع جنسية إباحية ونشرها بسرعة من خلال شبكة الإنترنت، الأمر الذي أجبر العديد من الشركات على إغلاق مزودات خدمة البريد الإلكتروني لديها، مما تسبب في خسائر كبيرة لها، للإشارة تمت متابعته وحكم عليه بالسجن لمدة (40) عاما وغرامة قدرها(470)ألف دولار[4] .

3-الهاتف النقال: ويسمى أيضا الهاتف المحمول أو الخلوي أو الجوال أو المتحرك، وهو عبارة عن:" أداة اتصال لاسلكية تعمل من خلال شبكة من أبراج البث موزعة لتغطي مساحة معينة، ثم تترابط عبر خطوط ثابتة أو أقمار صناعية"[5]. مع تطور هذه الأجهزة، أصبحت أكثر من مجرد وسيلة اتصال صوتي فهي حاسوب محمول حجمه بكف اليد، له وظائف كثيرة كالاتصال المرئي وتنظيم المواعيد واستقبال البريد الصوتي وإرسال واستقبال ملفات الفيديو والبريد الإلكتروني، وتصفح شبكة الإنترنت والتصوير واستعمال تقنية البلوتوث... إلخ. فقد تزايد عدد مستخدمي هذه الأجهزة

---

[1] محمود محمد لطفي صالح، المعلوماتية وانعكاساتها على الملكية الفكرية للمصنفات الرقمية-دراسة مقارنة، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر -الإمارات، 2014، ص185.

[2] عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنت-دراسة مقارنة، منشأة المعارف، القاهرة، مصر، ط1، 2010، ص66.

[3] *Myriam Quéméner et Joel Ferry, Op.Cit,p.36.*

[4] طارق ابراهيم الدسوقي عطية، المرجع السابق، ص541.

[5] التعريف موجود على الموقع الرسمي لموسوعة ويكيبيديا على الرابط الآتي:

https://ar.wikipedia.org/wiki/%D9%87%D8%A7%D8%AA%D9%81_%D9%85%D8%AD%D9%85%D9%88%D9%84، تاريخ الاطلاع:2015/03/29 على الساعة:08:53.

باستمرار خاصة بعد انتشار الهواتف النقالة الذكية، والتي أصبحت تقارب في خصائصها أجهزة الحاسوب، وصارت أداة لارتكاب كثير من الجرائم الإلكترونية مثل: جرائم الإباحية عبر الإنترنت جرائم السب والشتم والتشهير باستعمال الصور ومقاطع الفيديو...إلخ.

4-الشبكات المحلية والعالمية: يمكن تعريف شبكة الحاسوب على أنها:" نظام لربط جهازين أو أكثر باستخدام إحدى تقنيات نظم الاتصالات من أجل تبادل المعلومات والموارد والبيانات، كما تسمح بالتواصل المباشر بين المستخدمين"[1]. إذ يمكن أن تكون أجهزة الحاسوب في الشبكة قريبة جداً من بعضها مثل: أن تكون في غرفة واحدة وتسمى الشبكة في هذه الحالة بالشبكة المحلية *(LAN)، أو* يمكن أن تكون مكونة من مجموعة أجهزة في أماكن بعيدة مثل: الشبكات بين المدن أو الدول وحتى القارات وتسمى بالشبكات الإقليمية *(MAN)*، ويتم وصل هذه الشبكات في كثير من الأحيان بالإنترنت أو بالساتل *(Satellite)*، وتسمى الشبكة حينئذ شبكة عريضة *(WAN)*. في مقابل ذلك هناك ما يعرف بالشبكة الشخصية *(PAN)*، والتي تربط مجموعة أجهزة قريبة من المستخدم.

من جهة أخرى تعتبر شبكة الإنترنت *(INTERNET)* من أهم الشبكات، وتسمى أيضا بشبكة الشبكات، فهي تضم كافة أنواع الشبكات السابقة، فهي عبارة عن:" مجموعة من الحواسب المتصلة فيما بينها عن طريق أسلاك *(câbles)* أو دون أسلاك *(WIFI)* ، بحيث يمكن لأي منها الوصول إلى محتوى الآخر واستخدام موارده من تطبيقات وقواعد معطيات وغيرها من المعلومات"[2]. إن الهدف الدائم من الشبكة هو التشارك في المصادر *(Partage des ressources)*، وهي تتضمن الملفات وقواعد البيانات والبرامج...إلخ[3]. فقد تكون شبكة الإنترنت هدفا للجريمة كما في حالة الدخول غير المصرح به إلى الأنظمة المعلوماتية بقصد الاستيلاء أو تدمير بياناتها كما قد تكون أيضا أداة لارتكاب الجريمة الإلكترونية مثل: الاستيلاء على الأموال، وذلك بإجراء تحويلات غير مشروعة واستخدام التقنية في عمليات الاحتيال والتزوير...إلخ .لذا تعد هذه الشبكات مجالا خصبا لارتكاب شتى أنواع الجرائم الإلكترونية، كجرائم الاعتداء على نظام المعالجة الآلية للمعطيات، وجرائم المساس بحرمة الحياة الخاصة وغيرها كما سنرى ذلك لاحقا.

---

[1] فايز الظفيري، المقال السابق، ص494-495، للاستفادة أكثر، يرجى زيارة الموقع الرسمي لموسوعة ويكيبيديا على الرابط الآتي: *https://ar.wikipedia.org/wiki/%D8%B4%D8%A8%D9%83%D8%A9_%D8%AD%D8%A7%D8%B3%D9%88%D8%A8*، تاريخ الاطلاع:2015/03/29 على الساعة:09:30.

[2] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت(الجرائم الإلكترونية)-دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الإشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2007 ص20.

[3] المرجع نفسه، ص20.

بعدما تعرفنا على مفهوم الجريمة الإلكترونية وتصنيفها وأنواع المجنى عليهم فيها، وطبيعتها القانونية وخصائصها ومراحل وأساليب ارتكابها والأدوات المستعملة في ذلك، سنتطرق أيضا في المبحث الموالي إلى بنيانها القانوني، بما يمكّن المشرع الجزائري من رسم سياسة جنائية فعالة لمواجهتها.

المبحث الثالث: البنيان القانوني للجريمة الإلكترونية

يعتبر تحديد المشرع لمفهوم الجريمة وبنيانها القانوني، والذي يتطلب تبيان أركانها بدقة من الأمور الأساسية في سياسة التجريم والعقاب إعمالا لمبدأ شرعية التجريم والعقاب، خاصة فيما يتعلق بظهور هذه الجرائم المستحدثة التي لم يكن للمشرع سابق عهد بها نظرا لطبيعتها الخاصة، إذا تتم في بيئة افتراضية ويستعمل المجرم كل ما توصلت إليه التقنية المعلوماتية. ولكن قبل تناول البنيان القانوني للجرائم الالكترونية، لا بد من التطرق أولا إلى مدى خضوع المعلوماتية لجرائم الأموال ولنصوص الملكية الصناعية ولنصوص الملكية الأدبية والفنية بهدف تحديد طبيعة المال المعلوماتي في (المطلب الأول)، ثم نتعرف على أركان الجريمة الإلكترونية في (المطلب الثاني)، ثم نتناول مسألة الشروع والاتفاق الجنائي في الجرائم الإلكترونية وموقف المشرع الجزائري منهما في (المطلب الثالث)، وأخيرا ارتأيت أن أمد الباحث بصورة مختصرة عن تطور النظام القانوني للمشرع الجزائري المتعلق بمكافحة هذه الجرائم المستحدثة بهدف تسهيل فهم سياسته الجنائية بشقيها الموضوعي والإجرائي، وذلك في (المطلب الرابع).

المطلب الأول: مدى اعتبار المعلوماتية موضوعا لنصوص جرائم الأموال

نظرا لاختلاف طبيعة المال المعلوماتي عن مفهوم المال التقليدي، أثيرت بشأنه إشكالات عديدة، لذا قسمنا هذا المطلب إلى فرعين، نتطرق في (الفرع الأول) إلى الإشكالات التي أُثيرت بخصوص مدى خضوع المعلوماتية لجرائم الأموال، ثم نتناول في (الفرع الثاني) مدى خضوع المعلوماتية لنصوص الملكية الصناعية ولنصوص الملكية الأدبية والفنية.

الفرع الأول: مدى خضوع المعلوماتية لجرائم الأموال:

نظرا للطبيعة المستحدثة للجرائم الإلكترونية، فهي ترتكب في بيئة افتراضية تختلف تماما عن البيئة التقليدية، خلقت للفقهاء في جانبها الموضوعي كثيرا من المشكلات، ومنه يطرح التساؤل: إلى أي حد تعتبر التقنية المعلوماتية مالا؟.

أولا: مدى انطباق وصف المال على المعلوماتية: يقصد بالمال المعلوماتي الحاسوب بكل مكوناته، كما يمكن تعريف نظام الحاسوب بأنه: " مجموعة من الأجهزة المترابطة والتي تعمل معا من

خلال مجموعة من الأوامر والبيانات لتحقيق حل لمسألة معينة"[1]. وعليه يتكون الحاسوب من كيانين رئيسين هما :

1-الكيان المادي: يشمل مجموع الأجهزة المادية ويطلق عليها لفظ*(Hardware)* وتتألف من ثلاثة أقسام : يشمل القسم الأول وحدات الإدخال *(Input Units)*التي تنقل البيانات من خارج النظام إلى وحدة المعالجة والتخزين، كما يتكون القسم الثاني من وحدات المعالجة والتخزين(*Central Processing Unit)* التي تقوم بتنفيذ التعليمات على البيانات لمعالجتها وخزنها. وأخيرا وحدات الإخراج التي وظيفتها تسجيل النتائج وإخراجها إلى الوسط الخارجي*(Out put Units)*[2].

2-الكيان المعنوي: ويطلق عليه لفظ *(Software)*، ويقصد به مجموعة الأوامر والتعليمات الموجهة للحاسوب قصد القيام بوظائفه[3]، ويشيع تعبير البرنامج[4] أو البرمجيات للدلالة على الكيان المنطقي للحاسوب. فإذا كانت الأجهزة المادية للحاسوب لا تحتاج إلى نصوص خاصة لحمايتها جزائيا إذ تشملها نصوص الجرائم التقليدية، كجرائم السرقة والإتلاف...إلخ، فالأمر يختلف حينما نكون بصدد الكيان المعنوي للحاسوب، لأن جرائم الاعتداء على الأموال يشترط بشأنها عادة أن يكون موضوعها شيئا ماديا، وطبيعة الكيان المعنوي ليس كذلك[5]، مما يشكل لنا صعوبات بالغة، وعليه يُطرح التساؤل حول مدى اعتبار الكيان المعنوي للحاسوب مالا؟.

إن الأصل في الأشياء أن تكون مادية أي: يكون لها حيز محسوس كالأراضي المباني...إلخ ولكن نتيجة تقدم الفكر البشري وما صاحبه من اختراعات في شتى مجالات الحياة، بدأ ينشئ بالتدريج أشياء غير مادية ذات حيز غير محسوس نتج عنه حقوق مالية، علما بأن الأموال من وجهة النظر التقليدية لا ترد إلا على أشياء مادية، ولهذا كان تعريف المال بصدد جرائم الأموال بأنه " الحق المالي الذي يرد على الشيء، والشيء هو محل هذا الحق[6]. كما يندرج عادة في طائفة الأموال المادية *(biens matériel)* كل الأشياء التي لها وجود مادي، والتي تنتمي إلى عالم المادة، عكس الأموال غير المادية التي تتكون من قيم اقتصادية لا تتألف من عناصر مادية ولا يمكن حيازتها ولكنها مخصصة لمخاطبة الفكر[7].

---

[1] علي عبود جعفر، المرجع السابق، ص38.

[2] المرجع نفسه، ص39.

[3] محمد حماد مرهج الهيتي، جرائم الحاسوب-دراسة تحليلية، دار المناهج للنشر والتوزيع، عمان، الأردن، ط1، 2006، ص50.

[4] عرفت المادة (4/02) من (إ.ع.م.ج.ت.م) البرنامج المعلوماتي على أنه: "مجموعة من التعليمات والأوامر...".

[5] آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط1، 2006، ص15.

[6] عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، حق الملكية، دار إحياء التراث العربي، بيروت،ج8، 1952 ، ص9.

[7] محمد سامي الشوا، المرجع السابق، ص24.

إن سبب الحماية الجزائية المتميزة للأموال بصورتها المادية يتمثل في كونها ذات قيمة كبيرة على عكس الأموال المعنوية التي كان ينظر إليها على أنها عديمة القيمة أو ذات قيمة منخفضة وبالتالي اقتصرت النصوص التقليدية على حماية الأموال ذات الطبيعة الملموسة المادية دون المعنوية، من هذا يتضح لنا أن برامج وبيانات الحاسوب(الكيان المنطقي) لا تعتبر أموالا في نظر هذه النصوص التقليدية لانتفاء الصفة المادية عنها[1].

ومع التطورات المذهلة في مجال صناعة الحاسوب وبرامجه، لم تعد هذه النظرة مناسبة وانتشرت معه الأموال المعنوية بصورة كبيرة في شتى الميادين، مما أدى في بعض الأحيان إلى ارتفاع قيمتها عن قيمة الأموال المادية[2]، من هذه الأشياء المعنوية ذات القيمة الاقتصادية العالية برامج الحاسوب، فمن الناحية التقنية تثبت هذه البرامج على دعامة إلكترونية *(Support)* كالأقراص المرنة أو الأقراص المضغوطة...إلخ. فإذا كان البرنامج مستقل عن دعامته لا جدال فيه أنه شيء معنوي وبالتالي لا يصدق عليه وصف المال طبقا للمفهوم التقليدي للأموال الذي يشترط أن يكون محله شيئا مادي، أما إذا نقش البرنامج أو سُجل على دعامة إلكترونية ، فإن تلك الدعامة بما عليها من برنامج تصلح لأن تكون محلا لجرائم الأموال، على الرغم من أن قيمة تلك الدعامة منفصلة عن البرنامج ضئيلة جدا إذا ما قُورنت بقيمة البرنامج[3] ، فإذا وقع الاعتداء على البرنامج، فالأمر يختلف حيث يكون قد وقع على شيء معنوي، الذي لا بد من أن تثبت له صفة المال أولا، ثم يمكن أن نبحث بعدها في إمكانية وقوع جرائم الأموال عليه[4]، في هذا الصدد انقسم الفقه إلى قسمين:

1- **الاتجاه المؤيد لوصف المال على البرنامج:** يرى جانب من الفقه أن المعلومات صالحة لأن تكون محلا للاعتداء عليها طالما كانت هذه المعلومات تعكس الرأي الشخصي لصاحبها، مما يعني أنها من الحقوق اللّصيقة بشخصية صاحبها، وهذه المعلومات ذاتها هي موضوع هذا الحق ومن خصائصها القابلية للانتقال، إما بينها وبين صاحبها وإما بين صاحبها والغير، فالمعلومات باعتبارها نتاجا ذهنيا لمن يعطيها شكل المعلومة، فهي تعد محور العلاقات مثل تلك التي تنشأ بين المالك وبين ما يملك فيكون له نقلها وإيداعها وحفظها وتأجيرها وبيعها[5]. ومثال ذلك برامج الحاسوب، حيث عرفت المادة (4/02) من (إ.ع.م.ج.ت.م)، البرنامج المعلوماتي على أنه:" مجموعة من التعليمات

---

[1] عفيفي كامل عفيفي، المرجع السابق، ص111.

[2] المرجع نفسه، ص111.

[3] عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 1، 2009، ص06.

[4] آمال قارة، المرجع السابق، ص16

[5] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، مصر،2010، ص ص74-75.

والأوامر، قابلة للتنفيذ باستخدام تقنية المعلومات، ومعدة لإنجاز مهمة ما"، أو هو:" مجموعة البرامج والتعليمات المتعلقة بمعالجة مجموعة من المعطيات"[1] ، هذه البرامج ترتب حقوقا لصاحبها وتخول له إبرام عقود متعلقة بها مثل: الإيجار والبيع والحفظ وأي صورة أخرى من صور الاستغلال، لأن من خصائصها القابلية للانتقال[2].

إن هذا التطور في المفاهيم، هو الذي أدى بالفقه الحديث إلى إسباغ صفة المال على الشيء المعنوي، ليس فقط لوجود حق استئثار خاص عليها، وإنما أيضا بسبب القيمة الاقتصادية للشيء ذلك على أساس أن القانون الذي لا يسبغ صفة المال على الأشياء، يعد قانونا منفصلا عن الواقع [3]. فلقد بين الأستاذ كاتلا*(catala)*، أن المعلومة حينما يتم استحداثها فإنها تخص مالكها فيكون هو السيد عليها ويمكنه رفض إذاعتها، وإذا ما كانت متضمنة في برامج أو مخزنة على أي دعامة أخرى كانت مالا وقابلة للتملك ومرتبطة بصاحبها بعلاقة قانونية هي علاقة الحائز بما يحوزه[4].

وعليه تعتبر البرامج في جوهرها معلومات معالجة بطريقة ما، ولها قيمة اقتصادية فإنه يجب معاملتها على أنها مال، لذا يكون مقبولا أن يكون موضوع المال ليس فقط شيئا ماديا وإنما يكون شيئا معنويا أيضا مادامت له قيمة اقتصادية محمية قانونا ومنها برامج الحاسوب. وهذا ما اعتمده المشرع الحديث باعترافه لصاحب هذه المعلومات بالحق في الملكية الذهنية والأدبية...إلخ[5].

2- **الاتجاه المعارض لوصف المال على البرنامج:** يرى هذا الاتجاه عدم صلاحية المعلومات لأن تكون محلا للاعتداء عليها، حيث ذهب جانب من الفقه الفرنسي إلى أن المعلومة في حالتها المجردة لا تقبل التملك والاستئثار، وإن تداولها والانتفاع بها من حق الكافة دون تمييز، ومن ثم لا يمكن أن تكون محلا للملكية الفكرية[6]. ويفرق البعض الآخر بين المعلومات والبيانات التي تمت معالجتها إلكترونيا، فيرون أن المعلومات لها عنصر أساسي هو الدلالة لا الدعامة التي تجسدها فهي ذات طبيعة غير مادية، أما البيانات التي تمت معالجتها إلكترونيا، فتتحدد في كيان مادي يتمثل في نبضات أو إشارات ممغنطة يمكن تخزينها على وسائط معينة ونقلها واستغلالها وإعادة إنتاجها فضلا عن إمكانية قياسها. فهي إذن ليست شيئا معنويا كالحقوق والآراء والأفكار، بل شيئا له في العالم

---

1 *André Lucas et Autres, Op.Cit,p.303.*

2 علي عبد القادر القهوجي، المرجع السابق، ص75.

3 عفيفي كامل عفيفي، المرجع السابق، ص112.

4 هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص257.

5 علي عبد القادر القهوجي، المرجع السابق، ص76.

6 هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص ص256-257.

الخارجي المحسوس وجود مادي[1]. وفقا لهذا الرأي فإن المعلومات إذا لم تعالج آليا عن طريق الحاسوب لا تعتبر من قبيل الأموال الخاضعة للحماية الجنائية باعتبار أن هذه المعالجة تتم في صورة نبضات إلكترونية، مما يمكن القول بإمكانية تحولها من أموال معنوية إلى أموال مادية، الأمر الذي يخضعها للنصوص التقليدية لجرائم الأموال، ويأخذ نفس حكمها البيانات المخزنة سواء في برامج الحاسوب أو في ذاكرته، وبالتالي تتمتع بالحماية الجنائية المقررة لها[2].

3- **موقف المشرع الجزائري:** لقد أولى المشرع الجزائري عناية خاصة لحقوق الملكية الفكرية والأدبية، فلقد نص في المادة (44) من القانون رقم:16-01 المؤرخ في:2016/03/06 يتضمن التعديل الدستوري[3] على أن:" حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن، حقوق المؤلف يحميها القانون..."، وبذلك واكب المشرع التطور التكنولوجي الهائل الذي ظهر في مجال الحوسبة والاتصال، ومنها حماية برامج الحاسوب. تجلى ذلك في إصداره جملة من النصوص المتعلق بحقوق المؤلف والحقوق المجاورة كالأمر رقم:97-10 الذي وسّع من نطاق المصنفات المحمية إلى مصنفات الإعلام الآلي التي يقصد بها برمجيات الحاسوب وقواعد البيانات، حيث يُقصد بقواعد البيانات:" مجموعة أعمال أو معطيات أو عناصر في شكل ممنهج، يتم الدخول إليها بوسائل إلكترونية أو بأي وسائل أخرى"[4]. غير أن المشرع الجزائري لم ينص صراحة على حماية برامج الحاسوب.

ولتدارك هذا النقص التشريعي، قام المشرع بإصدار الأمر رقم:03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، والذي ألغى صراحة بموجب نص المادة (163) منه الأمر رقم:97-10 سالف الذكر، حيث أضفى الحماية القانونية على المصنفات الأدبية المكتوبة مثل: المحاولات الأدبية... وبرامج الحاسوب[5]، وبالتالي ساير المشرع الجزائري الاتجاه الفقهي المؤيد لوصف المال على البرنامج المعلوماتي باعتباره ذو قيمة اقتصادية جديرة بالحماية القانونية، تمهيدا لوضع سياسة جنائية مناسبة لمكافحة الجرائم الناشئة في مجال تكنولوجيا الإعلام والاتصال، وهذا ما قام به المشرع لاحقا.

---

[1] المرجع نفسه، ص249.

[2] آمال قارة، المرجع السابق، ص19.

[3] القانون رقم:16-01 المؤرخ في:2016/03/06، يتضمن التعديل الدستوري،(ج.ر) رقم:14 المؤرخة في:2016/03/07، ص ص3-37.

[4] *David FOREST et Gautier Kaufman, Droit de L'informatique, Gualino éditeur, Extenso édition, France,2010,p.29.*

[5] المادة (04) من الأمر رقم:03-05 يتعلق بحقوق المؤلف والحقوق المجاورة.

إن اعتبار المعلومات مالا، ستضاف حتما إلى مجموعة الأموال التي يحميها القانون الجنائي حيث لم تشترط هذه النصوص أن تقع جرائم الأموال على شيء مادي، وإنما على شيء مملوك للغير، وعليه يمكن تصور وقوع هذه الجرائم على المعلومات باعتبارها شيئا مملوكا للغير، إلا أنها شيء غير مادي، وخاصة بعد اضفاء صفة المال عليها. فهل تدخل برامج الحاسوب استنادا إلى هذه الصفة تحت مفهوم الشيء الذي يصلح محلا لجرائم الأموال؟.

ثانيا: مدى اعتبار المعلوماتية مالا بصدد جرائم الأموال: رأينا سابقا أن برامج الحاسوب وفقا للفقه الراجح ينطبق عليها وصف المال، بالمقابل ما مدى اعتبار برامج الحاسوب مالا بصدد بعض جرائم الأموال كجرائم السرقة، النصب وخيانة الأمانة، وتحطيم ملك الغير؟.

أ- مدى اعتبار المعلوماتية مالا بصدد جريمة السرقة: بالرجوع إلى (ق.ع.ج)، تنص المادة (1/350) على: "كل من اختلس شيئا غير مملوك له يعد سارقا..."، والاختلاس هو: "الاستيلاء على شيء بغير رضا مالكه أو حائزه"[1]، أو هو: "اختلاس مال منقول بنية تملكه"[2]، أو هو: "فعل الجاني الذي يؤدي إلى اغتيال وأخذ أو الاستيلاء على مال الغير أو أي شيء منقول بدون علم أو رضاء صاحب أو حائز هذا الشيء"[3] .

فمن خلال استقراء نص المادة سالفة الذكر، يتضح لنا أن المشرع لم يشترط صراحة ضرورة أن يكون المال موضوع الجريمة ماديا، مما يجعل وقوع جريمة السرقة على مال معنوي أمرا لا يصطدم بمبدأ شرعية التجريم والعقاب. فلقد استعمل المشرع مصطلح شيء دون قيد أو تخصيص وبالتالي يستوي لديه وقوع جريمة السرقة على أشياء مادية أو معنوية[4] .فعدم تحديد طبيعة الشيء أدى بالقول إلى امكانية تجريم اختلاس التيار الكهربائي على الرغم بأنه شيء غير ملموس، لأنه قابل للحيازة والتملك والنقل[5]. وهو ما نص عليه المشرع الجزائري بموجب المادة (2/350) من (ق.ع.ج) التي تنص على:...وتطبق نفس العقوبة على اختلاس المياه والغاز والكهرباء...". وعليه فإذا اتخذت الحقوق مظهرا ماديا، فإن هذه الأخيرة يصح أن يرد عليها الاختلاس، وعلى هذا الأساس يمكن القول

---

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط14،ج1، 2012، ص271.

[2] حسين فريجة، شرح قانون العقوبات الجزائري-جرائم الاعتداء على الأشخاص-جرائم الاعتداء على الأموال، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، ط2، 2009، ص188.

[3] محمد صبحي نجم، شرح قانون العقوبات الجزائري-القسم الخاص، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، ط5، 2004 ص116.

[4] علي عبد القادر القهوجي، المرجع السابق، ص78.

[5] عبد الله سليمان، دروس في شرح قانون العقوبات الجزائري-القسم الخاص، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، ط3 1990، ص218.

بأن الاستيلاء على البيانات المخزنة إلكترونيا باختلاس أوعيتها ووسائطها كالأشرطة والأسطوانات والأقراص الممغنطة والذاكرة الوميضية...إلخ، لا يثير مشكلة ويقع تحت طائلة فعل الاختلاس، لأن هذه الأوعية والوسائط المتعددة فضلا عن قيمتها الذاتية حتى وإن كانت ضئيلة لها كيان مادي محسوس[1].

غير أن جريمة السرقة بمفهومها السابق غير شائعة في مجال تقنية المعلومات، فيقوم المجرم المعلوماتي بالاستفادة من هذه التقنية بوسائل عديدة كنسخ المعطيات، أو الاتصال عن بعد بالبرامج أو ملفات البيانات المخزنة إلكترونيا، أو الدخول غير المشروع لقواعد البيانات بقصد الحذف أو التعديل ...إلخ، وعموما يمكن الاستيلاء على المعلومات دون وسائطها وأوعيتها وفق ثلاثة صور رئيسة[2]:

الصورة الأولى: الالتقاط الذهني للبيانات بصريا وحفظها في ذاكرة الإنسان: يرى بعض الفقه وقوع هذا الفعل تحت طائلة العقاب، فمع التحفظ بشأن صعوبة الإثبات، يمكن سرقة المعلومة من قبل من يقوم بدلا من النسخ، بقراءة مستند وتسجيل حفظ فحواه في ذاكرته.

الصورة الثانية: النسخ غير المشروع للبيانات المخزنة إلكترونيا: يتم تخزين البيانات المعالجة إلكترونيا في شكل نبضات كهربائية على أقراص مضغوطة أو مرنة أو صلبة، وفي كل الحالات يمكن نسخها، إلا أن هذه العملية تثير تردد الفقه والقضاء، ففي ألمانيا مثلا يجمع الفقه على أن المعلومات بحكم طبيعتها غير المادية لا تصلح محلا لجريمة السرقة، وهو نفس ما ذهب إليه الفقهاء في فرنسا بنفي الصفة المادية عن المعلومات. وعلى النقيض من ذلك، يقر رأي آخر حديث بأن الأشياء المعنوية تشملها الحماية التي يكفلها نص السرقة، على أساس أن المعلومات يمكن سرقتها إذا ما احتواها وعاء، و من ثمة يمكن سلب حيازتها ويجوز بالتالي أن تكون محلا للسرقة[3].

الصورة الثالثة: الالتقاط الهوائي للبيانات المعالجة أو المنقولة إلكترونيا: المعروف من الناحية التقنية أن الحاسبات الإلكترونية وداراتها الكهربائية تصدر أثناء تشغيلها إشعاعات كهرومغناطيسية يمكن التقاطها وترجمتها إلى بيانات مرئية على شاشة، كما يمكن أيضا اعتراض والتقاط البيانات المعالجة إلكترونيا أثناء نقلها بالموجات القصيرة من نهاية طرفية إلى نهاية طرفية أخرى[4].

---

[1] هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص ص229-230.

[2] آمال قارة، المرجع السابق، ص23-26.

[3] هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص ص 235-236.

[4] المرجع نفسه، ص250.

ومن هنا يُثار التساؤل أيضا حول مدى صلاحية الإشعاعات والموجات لأن تكون موضوعا للسرقة؟.

تعتبر القوى الطبيعية أو الصناعية الخاضعة لسيطرة الانسان والتي يمكنه توجيهها والاستفادة منها، من الأموال المنقولة تصلح لأن تكون محلا لجريمة السرقة، وانطلاقا من هذا المفهوم جرّمت تشريعات بعض الدول ومنها المشرع الجزائري سرقة الكهرباء وخطوط الهاتف والتدفئة والتبريد الصناعي[1]، أما الإشعاعات والموجات سواء كانت حاملة لإشارة مرمزة أم لا، فهي تنطلق في الفضاء ثم تضيع وبالتالي تفلت من سيطرة مرسلها، وعليه لا تشكل اعتداء على الحيازة ولا يمكن أن تكون محلا للسرقة، فلا تتحقق الحيازة إلا عند حرمان جميع أجهزة الاستقبال، وهذا أمر يصعب تحقيقه من الناحية العملية على أي شخص، إذ يتطلب ذلك أجهزة متخصصة يصعب إيجادها، وإن حدث الأمر تتحقق الحيازة وبالتالي تكون محلا لجريمة السرقة، والأمر سيان بالنسبة لالتقاط البيانات المعالجة إلكترونيا أثناء تناقلها إرسالا واستقبالا بين الأجهزة المعلوماتية[2].

وأخيرا يمكن القول بأن كل من الفقه والقضاء استقرا في تفسيرهما للنصوص المتعلقة بجريمة السرقة، على أن فعل الاختلاس يجب أن يرد على شيء مادي ملموس لكن مع ازدياد قيمة الأشياء المعنوية والتقدم العلمي الحاصل في مجال تقنيات المعلومات، أصبح بالإمكان وقوع فعل الاختلاس عليها، كما أن المشرع ذكر كلمة شيء دون قيد أو شرط ، وهذا ما دفع لاحقا لتجريم بعض الأشياء ليست ذات طبيعة مادية كالكهرباء مثلا[3]. وعليه لا يمكن اعتبار أن الأفكار والمعلومات بما فيها برامج الحاسوب طاقة ذهنية، فهي تقبل الحيازة عند إفراغها على دعامة بموافقة حائزها بواسطة كلمة السر، فهي تصلح لأن تكون محلا لجريمة السرقة بما لا يتعارض ومبدأ شرعية التجريم والعقاب ونظرا لأن المشرع لم يحدد صفة الشيئي من جهة، ومن جهة أخرى تعتبر هذه البرامج ذات قيمة اقتصادية ينطبق عليها وصف المال وأنها قابلة للتملك[4].

ب- مدى اعتبار المعلوماتية مالا بصدد جريمة النصب: تنص المادة (1/372) من (ق.ع.ج) على:" كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراقا مالية أو وعودا أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في

---

1 آمال قارة، المرجع السابق، ص27.

2 هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص255.

3 نايز نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر،2010، ص68.

4 أكثر تفاصيل في هذا الموضوع راجع، *Nidal El Chaer,Op.Cit,pp.55-63*

وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع أي شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20000 دج... ".وعليه يتكون الركن المادي لجريمة النصب حينما يستعمل الجاني وسائل التدليس المحددة بموجب نص المادة (372) سالفة الذكر، بهدف سلب مال الغير مثل: استعمال الأسماء أو الصفات الكاذبة، أو استعمال المناورات الاحتيالية[1].إن النشاط الإجرامي في جريمة النصب هو الاستيلاء على الحيازة الكاملة لمال مملوك للغير باستعمال إحدى الوسائل الاحتيالية المحددة في نص المادة سالفة الذكر، فإذا سلم الجاني للمجني عليه دعامة مادية مثبتا عليها أحد البرامج واستولى عليها الجاني فتتحقق الجريمة ولا مشكلة في ذلك[2].

ولكن يطرح التساؤل حول مدى إمكانية خضوع برامج وبيانات الحاسوب للنشاط الجرمي لجريمة النصب، في حالة إذا كان البرنامج مستقلا عن دعامته المادية؟. في هذا الشأن برز اتجاهان فقهيان هما [3]:

الاتجاه الأول: يرى عدم صلاحية برامج وبيانات الحاسوب لأن تكون موضوعا لجريمة النصب، بسبب عدم وجود نشاط مادي ملموس يحصل به التسليم والاستلام، وعلى فرض حدوث التسليم فإنه لا يترتب عليه حرمان المجني عليه من حيازة هذه البرامج التي تبقى تحت سيطرته.

الاتجاه الثاني: يقضي بصلاحية برامج وبيانات الحاسوب لأن تكون موضوعا لجريمة النصب واستدلوا على ذلك بأن النصوص الخاصة بهذه الجريمة تعطي لنا مجرد أمثلة على محل جريمة النصب، دون اشتراط أن يكون هذا المحل ذو طبيعة مادية أو معنوية.

ومنه يمكن القول بأن برامج وبيانات الحاسوب يمكن أن تكون موضوعا لجريمة النصب على أساس استغلال الجاني للتقنيات المذهلة في مجال تكنولوجيات الإعلام والاتصال، والتي تمكنه من استعمال الطرق الاحتيالية، كاتخاذ إسم أو صفة وهمية للتلاعب بالبيانات ويحولها كلها أو بعضها لصالحه، الأمر الذي دفع ببعض مشرعي الدول إلى النص صراحة على صلاحية النقود الكتابية أو الإلكترونية لأن تكون محلا لجرائم الأموال على الرغم من طبيعتها غير المادية[4].

---

[1] أكثر تفاصيل، راجع، حسين فريجة، المرجع السابق، ص ص257-263، وأيضا، محمد صبحي نجم، المرجع السابق، ص ص142-148.

[2] علي عبد القادر القهوجي، المرجع السابق، ص97.

[3] عفيفي كامل عفيفي، المرجع السابق، ص146.

[4] ومن الأمثلة على ذلك: المادة (2/282) من قانون العقوبات الكندي، والمواد(31و311و322) من قانون العقوبات الهولندي والمواد(140 و137و141) من قانون العقوبات السويسري، إضافة إلى قوانين الولايات المتحدة الأمريكية وانجلترا. بالنسبة للمشرع الفرنسي ابتدع نظرية "التسليم المعادل" والتي صيغت بمناسبة النصب على ضريبة المبيعات *(TVA)*، وعلى عدّاد موقف انتظار==

ج- مدى اعتبار المعلوماتية مالا بصدد خيانة الأمانة: بالرجوع إلى نص للمادة (376) من (ق.ع.ج) التي تنص على: "كل من اختلس أو بدّد بسوء نية أوراقا تجارية أو نقودا أو بضائع أو أوراقا مالية أو مخالصات أو أية محرّرات أخرى تتضمن أو تثبت التزاما أو إبراء لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير أجر بشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين وذلك إضرارا بمالكيها أو واضعي اليد عليها أو حائزيها، يعد مرتكبا لجريمة خيانة الأمانة ويعاقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من 500 الى 20.000دج...". نستنتج من نص المادة أن الاختلاس يقع على مال منقول سلم إلى الجاني بمقتضى عقد من عقود الأمانة الواردة على سبيل الحصر، إذ لا يجوز التوسع فيها، كما حددت المادة الأشياء التي تصلح لأن تكون محلا لهذه الجريمة وهي: الأوراق التجارية ، النقود، البضائع ،الأوراق المالية، المخالصات، وأية محررات أخرى تتضمن أو تثبت التزاما أو ابراء[1].

وعليه فإن إخضاع الاعتداءات الواردة على المال المعلوماتي إلى نصوص خيانة الأمانة يثير بعض المشكلات القانونية نظرا للطبيعة غير المادية للقيم في مجال الجريمة الإلكترونية. فبعدما رأينا سلفا أنه يمكن إصباغ وصف المال على برامج وبيانات الحاسوب نظرا لقيمتها الاقتصادية، فإنه يمكن أيضا أن يكون المال المعلوماتي موضوعا لجريمة خيانة الأمانة بصفتها بضائع، أو بوصفها سندات أو وثائق ترتب التزامات أو حقوق، هذا ما دفع القضاء الفرنسي بالتوسع في مفهوم فكرة البضائع *(marchandises)*، حيث يمكن تطبيقها ودون عناء على الجرائم الإلكترونية[2].

ث- مدى اعتبار المعلوماتية مالا بصدد جريمة التحطيم العمدي لملك الغير: كما رأينا سلفا تعتبر البرامج والبيانات من قبيل الأموال التي يجب أن تكون مشمولة بالحماية الجزائية، ومن المتصور أن تكون هذه البرامج والبيانات محل جريمة الإتلاف، مما ينتج عنه خسائر فادحة، وذلك عن طريق محوها أو إتلافها إما بصورة كلية أو جزئية باستخدام وسائل فنية توفرها المعلوماتية وبضغطة زر. فإذا كان محل الجريمة المكونات المادية للحاسوب كالشاشة ولوحة المفاتيح ...إلخ فهي تخضع للنصوص التقليدية لجريمة التحطيم العمدي لملك الغير، بشرط أن يؤدي التحطيم إلى

==السيارات والتليفون، والتي تلقفها الفقه كي يلاحق بها كافة أشكال النصب باستخدام الحاسوب، راجع، محمد سامي الشوا، المرجع السابق، ص ص131-132.

[1] عبد الله سليمان، دروس في شرح قانون العقوبات الجزائري، القسم الخاص، المرجع السابق، ص268.

[2] في هذا الصدد، تابع القضاء الفرنسي مندوب شركة متخصصة في بيع اللوحات الشهيرة بتهمة خيانة الأمانة، حيث غيّر مسار بطاقات عملاء الشركة بأن سلّمها لأحد العملاء بقصد نسخها بالتصوير، كما تمت متابعة شخص قام باختلاس وثائق محاسبتيه وشرائط ممغنطة باستخدام دعامة لتسجيل المسلسلات الإذاعية، راجع، محمد سامي الشوا، المرجع السابق، ص ص146-147.

التقليل من قيمتها الاقتصادية[1]. ولكن تُطرح المشكلة إذا كان محل الجريمة المكونات المنطقية للحاسوب كالبرامج والبيانات دون أن تتلف أوعيتها سواء انصب الاتلاف على جميع هذه البرامج أو بعضها. في هذا الصدد برز اتجاهان فقهيان هما[2]:

الاتجاه الاول: يري أصحابه بأنه لا تقوم جريمة الإتلاف نظرا لانتفاء الصفة المادية عن البرامج والبيانات وبالتالي فهي ليست مالا، إضافة إلى أن التدخل في وظائف واستخدامات الدعامات المادية المسجل عليها البرامج والبيانات لا يعتبر إتلافا لها.

الاتجاه الثاني: يرى أصحابه بأنه لا يوجد ما يحول دون وقوع هذه الجريمة على برامج وبيانات الحاسوب استنادا على حجج عديدة مثل[3]:

– اعتبار البرامج من قبل الأموال التي لها قيمة اقتصادية وخضوعها للتصرفات القانونية التي ترد على حق الملكية، والقول بغير ذلك يترتب عنه تجريدها من الحماية الجزائية.

– عدم تحديد المشرع لوسيلة معينة ترتكب بها هذه الجريمة، فمن الممكن اتجاه النشاط الإجرامي للجاني إلى البرنامج والدعامة المسجلة عليه معا، أو إلى البرنامج فقط دون الدعامة أو بواسطة الاتصال بالحاسوب عن بعد...إلخ.

– يمكن تصور أن تكون برامج وبيانات الحاسوب محلا لهذه الجريمة، ولو اقتصر الاتلاف عليها دون الدعامات المادية التي تحويها، وذلك عند تعريضها لقوى مغناطيسية من شأنها إفساد هذه البرامج والبيانات مما ينقص من قيمتها وبالتالي يعد إتلافا لها[4].

وبالرجوع إلى التشريع الجزائري نجد أن الاعتداء على الكيان المادي للحاسوب يمكن إخضاعه إلى نص المادة (1/412) من (ق.ع.ج)، والتي حددت الأشياء الخاضعة للإتلاف، حيث تنص على أنه: "كل من أتلف عمدا بضائع أو مواد أو محركات أو أجهزة أيًا كانت مستعملة في الصناعة وذلك بواسطة مواد من شأنها الإتلاف أو بأية وسيلة أخرى يعاقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من500 إلى 5000 دج....". فلقد حددت المادة على سبيل الحصر الأشياء المادية التي تصلح لأن تكون محلا لجريمة الاتلاف، وعليه وبما أن برامج الحاسوب يمكن إضفاء وصف المال عليها، لما لها من قيمة اقتصاديه تفوق أحيانا القيم المادية نفسها. يتضح لنا صلاحية أن تكون

---

[1] عفيفي كامل عفيفي، المرجع السابق، ص186.

[2] هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص314.

[3] علي عبد القادر القهوجي، المرجع السابق، ص103.

[4] عفيفي كامل عفيفي، المرجع السابق، ص189.

برامج الحاسوب وبياناته محلا لجريمة الإتلاف، على اعتبار مسايرة المشرع للتطور التكنولوجي الذي يلحق بالأشياء فيغيّر من طبيعتها.

نستخلص مما سبق، أن صلاحية البرامج لأن تكون محلا لجرائم الأموال، أمر يمكن استخلاصه من النصوص استنتاجا من عموميتها، ومن إمكانية إسباغ صفة المال بمفهومه الواسع على المعلومات باعتبارها ذات قيمة اقتصادية قابلة للتملك. وبذلك تقر صلاحيتها لأن تكون محلا لجرائم الأموال، أو أن يتدخل المشرع بإصدار تشريعات خاصة تجرم الاعتداء على المال المعلوماتي وهو ما قام به المشرع الجزائري كما سنرى لاحقا.

الفرع الثاني: مدى خضوع المعلوماتية لنصوص الملكية الصناعية والملكية الأدبية:

توفر التكنولوجيا الحديثة في مجال صناعة الحوسبة والاتصال، تقنيات هائلة في شتى مجالات الحياة، لذا اتجه الفقه الحديث إلى إصباغ وصف المال على برامج وبيانات الحاسوب، رغم أنه يشكل كيانا منطقيا، وهذا بسبب قيمته الاقتصادية التي تفوق في أحيان كثيرة القيمة المادية للأشياء. وكما رأينا سلفا أنه يمكن توفير حماية ولو نسبية لبرامج وبيانات الحاسوب بموجب النصوص التقليدية لجرائم الأموال، ولكن بالمقابل يُثار التساؤل حول مدى خضوعها لنصوص الملكية الصناعية ولنصوص الملكية الأدبية والفنية؟ وهل يمكن توفير الحماية الجزائية لها عن طرق هذه النصوص؟. بمعنى آخر هل برامج الحاسوب اختراع صناعي أم مصنف أدبي؟. وعليه سنتطرق أولا إلى مدى خضوع المعلوماتية لنصوص الملكية الصناعية، وثانيا إلى مدى خضوعها لنصـوص الملكية الأدبية والفنية.

أولا: مدى خضوع المعلوماتية لنصوص الملكية الصناعية: يعتمد تطور المجتمع على ما تمنحه القوانين من حرية فكرية تشمل كافة المجالات، حيث يضع المشرع ضمانات كفيلة بممارسة حرية الفكر بالنص عليها في وثيقة الدستور، ووضع عقوبات رادعة لمنع الاعتداء عليها. من هذا المنظور، يشمل قانون الملكية الصناعية مجالات عديدة كالعلامات التجارية وبراءة الاختراع والرسوم والنماذج...إلخ، سنتطرق بصفة موجزة إلى حماية برامج الحاسوب ضمن بعض هذه القوانين.

أ- **من خلال أحكام العلامات التجارية:** عرّف المشرع الجزائري العلامة التجارية بموجب نص المادة (1/02) من الأمر رقم:03-06 يتعلق بالعلامات[1] التي تنص على:"...العلامات كل الرموز القابلة للتمثيل الخطي، لا سيما الكلمات بما فيها أسماء الأشخاص والأحرف والأرقام والرسومات أو

---

[1] الأمر رقم:03-06 المؤرخ في:19 يوليو سنة 2003، يتعلق بالعلامات، (ج.ر) رقم:44 المؤرخة في:23 يوليو 2003، ص ص22-27.

الصور والأشكال المميزة للسلع أو توضيبها والألوان بمفردها أو مركبة التي تستعمل كلها لتمييز سلع أو خدمات شخص طبيعي أو معنوي عن سلع وخدمات غيره...". ويشترط في العلامة أن تكون مميزة وجديدة وغير مخالفة للنظام والآداب، ومسجلة لدى الجهة المختصة وهي المعهد الوطني الجزائري للملكية الصناعية[1].

كما تشمل الحماية القانونية للعلامة، تلك المدرجة ضمن التسجيلات الدولية وفي إطار الاتفاقيات الدولية التي انضمت إليها الجزائر كاتفاقية باريس لحماية الملكية الصناعية لسنة 1883 المعدلة ببروكسل سنة1925 ولندن سنة 1934 بموجب الأمر رقم: 75-02 المؤرخ في:1975/01/09. بالنسبة للبرنامج المعلوماتي، نجد أن كل برنامج يحمل اسما خاصا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية له، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى، فقد لجأ أصحاب البرامج إلى وضع الاسم مقترنا به مثل*(windows7)*. من ناحية أخرى رتب القانون جزاءات مدنية وجنائية في حالة الاعتداء على العلامة التجارية لا سيما في جرائم التقليد. كما يمكن ملاحظة محدودية مجال الحماية ضمن هذا الإطار بسبب اتساع مجال استخدام البرمجيات نظرا لاتساع رقعة التجارة الإلكترونية[2].

ب- من خلال أحكام براءة الاختراع: عرّف المشرع الاختراع بموجب المادة (02) من الأمر رقم: 03-07 يتعلق ببراءة الاختراع[3]على أنه :" فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية". كما يجب أن تتوافر في الاختراع شروطا بموجب نص المادة (03) من الأمر نفسه، كشرط الابتكار والجدة والقابلية للتطبيق الصناعي والمشروعية[4].عندما تتوفر هذه الشروط يتحصل المخترع على براءة الاختراع عن طريق وثيقة تمنح له من الجهة المختصة، تمكنه من حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة وبشروط معينة.

لكن بالمقابل هل تنطبق شروط الاختراع على برامج الحاسوب؟. بالرجوع إلى الفقه التجاري يرى ضرورة أن يكون الاختراع ذو صفة مادية حتى يتمتع بالحماية القانونية، وكل ذلك في إطار شرط القابلية للاستغلال الصناعي أي: أنه له بعد مادي بحت، وهذا ما يفرّق على أساسه الفقه التجاري بين الابتكار الصناعي والمصنفات الأدبية[5]، فمن جهة يتجرد الكيان المنطقي من أي طابع صناعي

---

[1] زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر،2011، ص96.

[2] المرجع نفسه، ص97.

[3] الأمر رقم:03-07 المؤرخ في:2003/07/19 يتعلق ببراءات الاختراع، (ج.ر) رقم:44 المؤرخة في:2003/07/23، ص ص27-35.

[4] لأكثر تفاصيل حول شروط الاختراع، راجع، بشرى النية، المقال السابق، ص ص122-126.

[5] عفيفي كامل عفيفي، المرجع السابق، ص54.

وبالتالي لا ينطبق عليه تعريف المنتج الجديد المستحق للبراءة، بسبب أنه لا يتمثل في جسم محدد حتى ولو اتصل بالدعامة المادية التي تحويه، فإن هذا ليس كافيا لاعتباره منتجا، ومن جهة أخرى هناك صعوبة في تقييم عنصر الجدة للكيان المنطقي للحاسوب من المبرمجين والمتخصصين أنفسهم ناهيك عن غياب قواعد عامة تتيح لهم عملية التقييم[1].

بناء على ما سبق، نستنتج أن برامج الحاسوب غير مؤهلة في حد ذاتها لتكون محلا لبراءة الاختراع بسبب التعارض بين طبيعة البرنامج كعامل ذهني منطقي هدفه معالجة البيانات والمعلومات، وبين النظام القانوني الذي يفرض شروطا لا تتوافق وطبيعته لمنح براءة الاختراع. لذلك تم استبعاد أحكام براءة الاختراع كوسيلة قانونية لحماية برامج الحاسوب، وذلك بموجب نص المادة (6/07) من الأمر رقم:03-07 سالف الذكر:" لا تعد من قبل الاختراعات في مفهوم هذا الأمر...برامج الحاسوب..."[2].

وتجدر الإشارة إلى أنه يمكن استثناء الحصول على براءة الاختراع بخصوص برامج الإعلام الآلي في حالتين هما:

– أن يكون البرنامج جزءا من ذاكرة الحاسب نفسه مثل: البرنامج المبني.

– أن يكون البرنامج جزء من وسيلة صناعية جديدة: حيث يستخدم البرنامج في تحقيق إحدى مراحلها، فالحماية تبقى رهينة توفر الشرطين المذكورين وقد ثبت صعوبة توفرها، وبالنتيجة ثبت تعذر الحماية بموجب قانون براءة الاختراع[3].

إذا كانت برامج الحاسوب غير مؤهلة في حد ذاتها لتكون محلا لبراءة الاختراع ، فهل يعتبر قانون الملكية الفكرية والأدبية في التشريع الجزائري إطارا مناسبا لحماية برامج الحاسوب؟. هذا ما سنراه بصفة موجزة فيما يأتي.

ثانيا: مدى خضوع المعلوماتية لنصوص الملكية الأدبية والفنية: إن حماية حقوق المؤلف ضرورة لابد منها، حيث اهتمت جل التشريعات الحديثة بحماية هذا الحق، وذلك لتشجيع الإبداع الفكري البشري وحثه على تقديم الأفضل دون الخوف من عمليات السرقات الأدبية التي تطال منتجاتهم. إن مضمون حق صاحب براءة الاختراع وحق المؤلف، هو الدافع على تقرير الحامية القانونية لصاحب الحق بمختلف صورها، فمتى عبّر عن فكرة الاختراع أو المؤلف بصورة تتجاوز

[1] محمد سامي الشوا، المرجع السابق، ص33.

[2] زيدان زيبحة، المرجع السابق، ص91 ، راجع أيضا، بشرى النية، المقال السابق، ص ص127-128.

[3] فاطمة زهرة بوعناد، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، قسنطينة، الجزائر، العدد1 ،2013، ص66.

ذهن صاحبها، فقد صارت معلومة علمية أو فنية أو صناعية أو غيرها، وحينئذ فهي مال يتمتع صاحبها بسلطة الاستغلال أو السحب أو التعديل[1]. من هذا المنطلق نظم المشرع الجزائري هذه الحقوق ضمن قانون الملكية الأدبية والفنية بمقتضى نصوص عديدة تعديلا وإلغاء، كان آخرها صدور الأمر رقم: 05/03 المؤرخ في 2003/07/19 يتعلق بحقوق المؤلف والحقوق المجاورة، تماشيا في ذلك مع الحركة التشريعية العالمية التي اهتمت بحماية البرمجيات عن طريق حقوق الملكية الفكرية والأدبية منذ اتفاقية باريس لسنة 1883 التي نتج عنها إبرام اتفاقيات عديدة بين الدول، مثل الاتفاقية المعروفة باسم التريبس*(TRIPS)*[2] المتعلقة بحقوق الملكية الفكرية، والتي تشرف على تطبيقها المنظمة العالمية للملكية الفكرية *(WIPO)*[3]، حيث تنص المادة (1/10) من هذه الاتفاقية:" تتمتع برامج الحاسب الآلي (الكمبيوتر)، سواء أكانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن(1971)...[4].

---

1 عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دار النهضة العربية، مصر، ط2 1995، ص22.

2 اتفاقية تريبس: هو اتفاق بخصوص الجوانب التجارية لحقوق الملكية الفكرية تديره المنظمة العالمية للملكية الفكرية *(WIPO)*، تأسّست بموجب اتفاقية مراكش بتاريخ: 1994/04/15 من طرف الدول الأعضاء في المنظمة العالمية للتجارة، وتم تطبيقها في سنة 1995. تعتبر اتفاقية تريبس الأولى التي أقرت إجراءات تحمي حقوق الملكية الفكرية، ومنها برامج الحاسوب كما أنها تعكس قناعات الدول حول حماية حقوق التأليف والنشر وغيرها من كافة أشكال الاعتداءات. كما تهدف عموما إلى تسهيل الطرق أمام التجارة الدولية، بما في ذلك حماية الملكية الفكرية بصورة فعالة، خاصة باعتماد المواد من(41-01) من اتفاقية برن لسنة 1971، كما تهدف أيضا الى تطوير النشاط في برامج الحاسوب ضمن سياسات وطنية ومن خلال حمايتها بموجب قوانين الملكية الفكرية، فكان لهذه الاتفاقية نتائج ايجابية على حماية حق المؤلف، وتجلى ذلك في زيادة الاتجار ببرامج الكمبيوتر المشروعة وانخفاض عدد عمليات القرصنة، حيث تقلص عددها في دولة الإمارات في سنة واحدة من 88% إلى 72%. وهكذا جمعت اتفاقية التريبس أحكام الاتفاقيات الدولية الرئيسية في مجال الملكية الفكرية ضمن وثيقة واحدة، فحققت الترابط فيما بينها، بعد أن كانت هذه الأحكام متفرقة ومبعثرة في الاتفاقيات الدولية المختلفة. كما ألزمت جميع الدول الأعضاء في منظمة التجارة العالمية بتطبيق أحكامها بغض النظر عن انضمامها إلى هذه الاتفاقيات الدولية من عدمه. ولم تقف اتفاقية التريبس عند حد الإحالة إلى أحكام الاتفاقيات الدولية المبرمة في شأن الملكية الفكرية ، بل أنها اعتبرت أحكام هذه الاتفاقيات هي نقطة البداية التي انطلقت منها نحو تدعيم وترسيخ حقوق الملكية الفكرية، فاستحدثت أحكاماً جديدة لم تنظمها الاتفاقيات الدولية من قبل كما طورت أحكامها من أجل تدعيم حقوق الملكية الفكرية وترسيخها على المستوى الدولي، راجع، نعيم مغبغب، حماية برامج، المرجع السابق، ص ص21-22.

3 منظمة *(wipo)*: هي المنتدى العالمي للخدمات والسياسة العامة والتعاون والمعلومات في مجال الملكية الفكرية، وهي وكالة من وكالات الأمم المتحدة التي تمول نفسها بنفسها. يبلغ عدد أعضائها 188 دولة، مهمتها الاضطلاع بدور ريادي في إرساء نظام دولي متوازن وفعّال للملكية الفكرية يشجّع الابتكار والإبداع لفائدة الجميع. وترد هيئاتها الرئاسية وإجراءاتها التنظيمية في اتفاقية الويبو التي أنشأت بموجبها منظمة الويبو سنة 1967، للاطلاع أكثر يرجى زيارة الموقع الرسمي للمنظمة على الرابط الآتي:*http://www.wipo.int/about-wipo/ar/what_is_wipo.html*، تاريخ الاطلاع:2015/10/24 على الساعة:09:24.

4 وعليه تتمتع برامج الكمبيوتر، سواء كانت شيفرة مصدرية أو شيفرة مستهدفة بالحماية باعتبارها مصنفات فنية بموجب اتفاقية برن (1971). إذ تؤكد هذه المادة على وجوب حماية برامج الحاسب الآلي باعتبارها من حقوق المؤلف على أن تطبق عليها أيضاً أحكام اتفاقية برن في شأن المصنفات الفنية. كما تنص الاتفاقية على تطبيق المفهوم العام لاصطلاح الحماية المعمول به منذ خمسين سنة==

في هذا الشأن وبعد انضمام الجزائر سنة 1975 لاتفاقية باريس المعدلة، واستكمالا لهذا المسار ونتيجة للتطور التكنولوجي المتلاحق الذي صاحبه تطور تقني هائل في مجالات عديدة، انظمت الجزائر بتحفظ لاتفاقية برن لحماية المصنفات الأدبية والفنية لسنة 1882 والمعدلة لاحقا(1). وقصد تحديد مدى خضوع المعلوماتية للحماية المقررة بمقتضى هذا القانون، وجب التطرق قبل ذلك إلى نقطتين أساسيتين، من جهة مدى اعتبار البرنامج كموضوع من موضوعات حق المؤلف، ومن جهة أخرى مدى خضوع برامج الحاسوب للنشاط الإجرامي لجرائم التقليد .

أ- مدى اعتبار برنامج الحاسوب كموضوع من موضوعات حق المؤلف: في هذا الصدد

اختلف الفقه حول مدى اعتبار البرنامج مصنفا فكريا يخضع للحماية الجزائية لقوانين الملكية الفكرية والأدبية، وبرز رأيان في هذه المسألة:

- **الرأي المؤيد:** يرى أصحاب هذا الرأي بإمكانية اضفاء الحماية القانونية لبرامج الحاسوب وذلك اعتمادا على حجج منها، أن البرنامج يمثل طريقة للتعبير عن الأفكار، كما أن البرامج ما هي إلا تعبيرات التخاطب مع مستعملي الحاسوب، فيكتب البرنامج بأحد لغات البرمجة في صورة أولية، ثم بعد ذلك يحول إلى لغة الآلة التي تقرؤه، ثم تخرجه للمستعمل للاستفادة منه(2).كما أن إعداد برامج الكمبيوتر يتيح مجالا للابتكار باستثناء بعض البرامج البسيطة، إضافة إلى أن معاهدة برن تعتبر وفقا لنص المادة (1/02) برامج الحاسوب محررات باعتبارها أوعية تتمتع بالحماية القانونية حتى ولو كانت محررات علمية أو ذات غاية تجارية باعتبارها ابتكارا ذهنيا(3).
- **الرأي المعارض:** يشكك أصحاب هذا الرأي في خضوع الكيان المنطقي للحاسوب للحماية بموجب حق المؤلف نظرا لاعتبارات عديدة نذكر منها، إمكانية قيام شخص عاد يتمتع بقدر معقول في مجال تقنية المعلومات بإجراء تعديل بسيط على الكيان المنطقي للحاسوب، ومن ثمة يطالب بإضفاء الحماية القانونية له باعتباره مبتكرا له، كما أن الكيان المنطقي للحاسوب يفتقد لشرط الابتكار

==على برامج الكومبيوتر. في الصدد نفسه، نصت المادة (2/10) من الاتفاقية على حماية قواعد البيانات وغيرها من البيانات المجمعة أو المواد الأخرى على النحو المكفول لحقوق المؤلف، وحتى وإن كانت قواعد البيانات هذه تتضمن معلومات لا تشملها حماية حقوق المؤلف. ويشترط لتمتع قواعد البيانات بحق حماية حقوق المؤلف أن تمثل إبداعات فكرية، كما يؤكد مضمون هذه المادة وجوب توفير الحماية لقواعد البيانات بصرف النظر عن الشكل المقترن بها سواء أكانت في شكل مقروء آليا أو أي شيء آخر، للاطلاع أكثر على نصوص الاتفاقية، يرجى زيارة موقع المنظمة على الرابط الآتي: *http://www.wipo.int/treaties/ar/ip/wct/* ، تاريخ الاطلاع:2015/10/24 على الساعة:09:07.

[1] المرسوم الرئاسي رقم:341/97 المؤرخ في:1997/09/13، يتضمن انضمام الجمهورية الجزائرية الديمقراطية الشعبية، مع التحفظ، الى اتفاقية برن لحماية المصنفات الأدبية والفنية المؤرخة في:1886/09/09...،(ج.ر) رقم:61 المؤرخة في:1997/09/14، ص ص8-35

[2] آمال قارة، المرجع السابق، ص70.

[3] محمد علي العريان، المرجع السابق، ص198.

الذي لا يعبّر عن شخصية مبتكره، ناهيك عن الطبيعة الخاصة للكيان المنطقي الذي يتميز عن غيره من الكيانات وينفرد بخصائص ذاتية[1].

تكمن العبرة في استحقاق برامج الحاسوب حماية حق المؤلف من عدمها، في مدى توافر شروط المصنف المحمي في برامج الحاسوب كشرط الابتكار ومدى مساهمته في إضافة فكرة جديدة ، وشرط التجسيد أو التثبيت على دعامة مادية مما يسمح في الأخير بتصنيف هذا المؤلف واضفاء الحماية عليه[2]. إن برامج الحاسوب تعد ثمرة من أبدعه ويتمتع بالطابع الشخصي لمؤلفه، فالابتكار شرط ضروري لحماية البرامج كمصنف أدبي، سواء كان البرنامج بسيطا أو ذو قيمة عالية أو فائدة محددة[3].

بالرجوع إلى المشرع الجزائري، وبسبب الاستجابة لشروط المنظمة العالمية للتجارة *(OMC)* من جهة، ومن جهة أخرى تطبيقا لنصوص الاتفاقيات المبرمة في هذا الشأن كالتصديق على نصوص (إ.ع.م.ج.ت.م) التي تنص في المادة (17) منها على تجريم انتهاك حقوق المؤلف والحقوق المجاورة. وذلك اذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي. في هذا الشأن اعتبر المشرع برامج الحاسوب ضمن المصنفات الأدبية والفنية الجديرة بالحماية وهذا بموجب نص المادة (04) من الأمر رقم:05/03 سالف الذكر التي تنص على أنه:" تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي:...برامج الحاسوب..." كما لصاحبه الحق في استغلال برنامجه بشتى الطرق دون غيره وإبلاغه للجمهور بأي منظومة معالجة معلوماتية ويترتب عن ذلك وفق لأحكام المادة (27) من الأمر نفسه حقوق مادية بالاستغلال التجاري له ولورثته.

من جانب آخر، أقّر المشرع الحماية نفسها بشأن قواعد البيانات وهذا بموجب نص المادة (05) من الأمر نفسه التي تنص على:" تعتبر أيضا مصنفات محمية الأعمال الآتية...المجموعات والمختارات من المصنفات، مجموعات من مصنفات التراث الثقافي التقليدي وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى...".

وكخلاصة تتطلب البرمجيات لحمايتها توافر شروط على درجة كبيرة من الأهمية كشرط الابتكار الذي يحدد طبيعتها وقيمتها الفنية ومدى استحقاقها للحماية، ثم يأتي شرط إيداعها لدى الجهة

---

[1] محمد سامي الشوا، المرجع السابق، ص38.

[2] بشرى النية، المقال السابق، ص167.

[3] خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء قانون حماية الملكية الفكرية –دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2005، ص71.

المختصة وفقا لنص المادة (03) من الأمر نفسه[1]. وعليه وسّع المشرع الجزائري من قائمة المؤلفات المحمية، ومنها برامج الحاسوب وقواعد البيانات، وأقر لها مدة حماية محددة بخمسين(50) سنة بعد وفاة المبدع وفقا لنص المادة (54) من الأمر رقم:03-05 سالف الذكر، وهي مدة طويلة ليست في مصلحة المجتمع وتمكّن أصحاب المؤلفات المعلوماتية من احتكار هذه المعرفة التكنولوجية، كما يتناقض أيضا مع تطبيقات الإعلام الآلي التي يجب أن تكون قصيرة المدة فهي تمتاز بالتطور الدائم.

من جانب آخر، نص المشرع على تشديد العقوبات الناجمة عن المساس بحقوق المؤلف لا سيما في مجال تأليف المصنفات المعلوماتية. ولكن ما مدى خضوع برامج الحاسوب للنشاط الإجرامي لجرائم التقليد؟.

ب- مدى خضوع برامج الحاسوب للنشاط الإجرامي لجرائم التقليد: لم يعرف المشرع الجزائري جريمة التقليد، وبالرجوع إلى الفقه عرفها بعضهم بأنها: "نقل مصنف لم يسقط في الملك العام من غير إذن مؤلفها"[2]، وكما رأينا سلفا، أدمج المشرع الجزائري برامج الحاسوب وقواعد البيانات ضمن قائمة المصنفات المحمية عن طريق القانون المتعلق بحق المؤلف، فإن أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج يشكل فعلا من أفعال التقليد، وقد نص المشرع الجزائري في الأمر رقم: 03-05 على جريمة التقليد والجرائم المشابهة لها – سنتطرق إليها لاحقا بالتفصيل- بموجب نصوص المواد (151 - 153)، إذا تنص المادة (151) على جنحة التقليد في حالة الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف، واستنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة. كما نصت المادة (152) من الأمر نفسه على: "يعد مرتكبا لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الأداء عن طريق التمثيل أو الأداء العلني...أو صورا أو أصواتا أو بأي منظومة معالجة معلوماتية".

لقد حددت المادتان (151) و (152) مجموعة السلوكيات المادية التي تشكل الركن المادي لجنحة تقليد المصنفات، ومنها برامج الحاسوب كالكشف غير المشروع عنها، واستيراد أو تصدير نسخ مقلدة للبرمجيات، وبيع نسخ مقلدة لمصنف أو أداء، أو تأجير برمجة مقلدة أو عرضها للتداول، أو استنساخها في شكل نسخ مقلدة، سواء كان الاستنساخ في صورته المعروفة مثل: نسخ قرص*(CD)* إلى قرص آخر*(Gravure de CD)*، أو بأي وسيلة استنساخ أخرى. في الصدد نفسه، اعتبر المشرع الجزائري في نص المادة (2/27) من الأمر نفسه بأن المؤلف أو مالك الحقوق المادية على

---

[1] بن زيطة عبد الهادي، المرجع السابق، ص43.

[2] جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية، المرجع السابق، ص144.

المصنف، هو الوحيد المخول دون غيره بإجراء نسخ من المصنف وبأي وسيلة كانت[1]. وعليه يتمثل النشاط الجرمي في الاعتداء على أي حق من حقوق المؤلف أيا كانت صورته ومهما كانت جسامته فمثلا تشكل جريمة تقليد البرمجيات في فرنسا أكثر من 57%، وفي لبنان ما نسبته 83%[2].

وكنتيجة يمكن القول: بأن أحكام العلامات التجارية وقانون الملكية الأدبية والفنية يعترفون لبرامج الحاسوب وقواعد البيانات بصفة المصنف المحمي، غير أنها لا تزال قاصرة على ضمان الحماية الجزائية اللاّزمة بسبب الطفرة التكنولوجية الهائلة في مجال صناعة الحوسبة والاتصال واتساع مجالات تطبيقهما، وما ينتج عن ذلك من جرائم إلكترونية مستحدثة تمس الأشخاص والأموال على حد سواء. لذا كان لزاما على المشرع استحداث نصوص تجريميه خاصة بمكافحة الجرائم الإلكترونية وذلك ما اعتمده المشرع الجزائري بتعديله لقانون العقوبات باستحداث فصل خاص بالاعتداءات على أنظمة المعالجة الآلية للمعطيات، ناهيك عن استكمال هذه المنظومة التجريمية بنصوص خاصة سنتطرق إليها لاحقا بالتفصيل.

المطلب الثاني: أركان الجريمة الإلكترونية

مما لا شك فيه أن الجرائم الإلكترونية لا تختلف عن أية جريمة تقليدية أخرى بخصوص توفر أركانها، فبالإضافة إلى ضرورة توفر الركن الشرعي حفاظا على مبدأ شرعية التجريم والعقاب الذي يفيد النهي عن أمر أو الاتيان بفعل أمر وتقرير عقوبة لمن يخالف النهي بالارتكاب أو لمن يخالف الأمر بالامتناع[3]. وعليه يعتبر النص القانوني هو مصدر التجريم، وهو "المعيار الفاصل بين ما هو مباح وبين ما هو منهى عنه تحت طائلة الجزاء"[4]، كما نشير إلى أننا نستبعد الحديث عن الركن الشرعي لوضوح الأمر. من جانب آخر، يجب أن يتوفر أيضا الركن المادي الملموس الذي يعبر عن السلوك الإجرامي للفاعل والذي يثير إشكالات عديدة في هذا النوع المستحدث من الجرائم(الفرع الأول)، كما يجب أن يتوفر أيضا الركن المعنوي الذي يعبر عن القصد الجنائي للمجرم بخصوص علمه وإرادته للقيام بالعمل المجرم، هذا ما سنتناوله في (الفرع الثاني).

الفرع الأول: الركن المادي:

لا يعاقب القانون الجنائي على الأفكار والنوايا السيئة ما لم تخرج إلى الوجود الخارجي بفعل أو عمل، وهذا الفعل أو العمل الخارجي الذي يعبر عن النية الجنائية أو الخطأ الجزائي يسمى بالركن

1 عبد الهادي بن زيطة، المرجع السابق، ص ص78-79.

2 زينات شحادة، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، دار المنشورات الحقوقية، لبنان، 2006، ص ص76-77.

3 علي عبود جعفر، المرجع السابق، ص127.

4 أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط11، 2012، ص58.

المادي للجريمة[1]، وعليه يقوم الركن المادي في الجريمة التامة على ثلاثة عناصر هي: السلوك الإجرامي الذي يقع من الجاني والنتيجة الضارة المترتبة عن هذا السلوك والعلاقة السببية بين السلوك المجرم والنتيجة المحققة، كما أنه يختلف من جريمة لأخرى. بالمقابل تبرز لنا مشكلة بخصوص تحديد طبيعة الركن المادي في الجرائم الإلكترونية، فهي تتم باستخدام الحاسوب كأداة، أو قد يكون الحاسوب هو نفسه هدفا لها[2].

يتمثل السلوك الإجرامي في النشاط المادي الخارجي للجريمة، أو هو حركة الجاني الاختيارية والتي يترتب عليها تغيير في العالم الخارجي، كما يتخذ السلوك الإجرامي إحدى الصورتين: **أ- سلوك إيجابي** : يتمثل في حركة عضوية إرادية تقوم على الإدراك والتمييز وحرية الاختيار في القيام بعمل ينهى القانون عن ارتكابه كالسرقة مثلا. فالسلوك الإجرامي في جريمة السرقة، يتمثل في نقل حيازة المال من مالكه الأصلي إلى حيازة الجاني، وهذا دون علم ورضا المجني عليه، وقد يأتي هذا السلوك في صورة بسيطة أو معقدة أو بصورة وقتية محددة في الزمان أو مؤقتة[3]. إن السلوك الإجرامي يختلف حسب نوع الجريمة، فهو في الجريمة البسيطة فعل واحد لا يلزم تكراره كجريمة السرقة، بينما يكون متكررا على مراحل في الجرائم متعددة الأفعال، ولكن تجمعه وحدة الغرض كسرقة منزل على مراحل متعاقبة، وفي الجريمة الوقتية يبدأ وينتهي بمجرد تمامه، بينما هو قائم ومتجدد ومستمر في الزمن في الجرائم المستمرة كحيازة سلاح دون رخصة[4].

ب- سلوك سلبي (الإمتناع): خلافا للقاعدة العامة فقد يأمر المشرع بالإقدام على عمل معين ويقرر العقوبة لمن يمتنع عن إتيانه، متخذا بذلك موقفا سلبيا عما أمر به القانون مثل: امتناع شاهد عن الحضور أمام محكمة الجناية، وعدم الإبلاغ عن جناة...إلخ[5]، ويشترط أن يكون في استطاعة الممتنع القيام بذلك الواجب أو الالتزام، وأن مصدر هذا الإمتاع هو الإرادة.

أما بخصوص الجرائم الإلكترونية، ونظرا لما توفره تكنولوجيا الحوسبة والاتصال من تقنيات مذهلة تتميز بالسرعة والدقة وإمكانية الإفلات من الملاحقة في هذه البيئة الرقمية، فالركن المادي فيها عادة ما يبدأ بضغطة زر على لوحة المفاتيح أو بلمسة على شاشة الحاسوب أو الهاتف النقال، مثل: قيام المجرم الإلكتروني بالدخول للشبكة والتعارف على أشخاص عن طريق انتحال شخصية كمستثمر أو تاجر قصد الحصول على أموالهم عبر شبكة الإنترنت. أو عند قيام المجرم ببرمجة فيروس وإرساله

---

1 المرجع نفسه، ص97.

2 عماد مجدي عبد الملك، المرجع السابق، ص36.

3 حنان ريحان مبارك المضحكي، المرجع السابق، ص86.

4 عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر، المرجع السابق، ص139.

5 أحسن بوسقيعة، الوجيز في القانون الجزائي العام، المرجع السابق، ص ص98-99.

سواء لتحميل بيانات أو تدميرها، أو إرسال ملف فيديو أو رسائل نصية تمس بشخص المتلقي عبر البريد الإلكتروني أو الهاتف النقال[1].

إن السلوك الاجرامي في الجريمة الإلكترونية يرتبط عموما بالمعلومة المخزنة على الحاسوب أو تلك التي يتم إدخالها ، فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك أو إساءة استخدام بطاقات الائتمان[2]. فالجريمة الإلكترونية يتطلب ارتكاب ركنها المادي منطق تقني أي: توافر القدر اللازم من العلم والادراك لاستخدام هذه التقنية، فهي تتم عبر شبكة الإنترنت أو باستخدام نظام المعالجة الآلية للمعطيات مثل المصرفي الذي ينوي سرقة مبالغ مالية من المصرف الذي يعمل فيه باستخدام الإنترنت، ثم الدخول لشبكة المصرف عبر مزودات مجهولة عن طريق الاستعانة ببرامج اختراق توفرها مراكز للهاكرز[3].

وبناء عليه يظهر لنا مدى صعوبة تحديد الركن المادي في الجرائم الإلكترونية، والذي يختلف من جريمة لأخرى، كان لزاما على المشرع الجزائري أثناء وضعه لسياسته الجنائية لمكافحة هذا النوع المستحدث من الجرائم تحديد هذا الركن وبدقة، قصد الإحاطة بأكبر عدد ممكن من هذه الجرائم وضمانا لعدم إفلات المجرم المعلوماتي من العقاب في هذه البيئة الافتراضية. فقام بتعديل قانون العقوبات بموجب القانون رقم:04-15 المؤرخ في: 2004/11/10 يعدل ويتمم الأمر رقم: 66-156 المؤرخ في: 8 يونيو 1966 والمتضمن قانون العقوبات، أين أضاف قسم سابع مكرر عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من(394 مكرر - 394 مكرر 7)، أين نص على الجرائم الماسة بالأنظمة المعلوماتية، وإن كانت تختلف في أركانها وعقوباتها تبعا لاختلاف نوع الجريمة، إذ يتمثل الركن المادي عموما في أشكال الاعتداء على نظم المعالجة الآلية للمعطيات مثل: جريمة الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، أو جريمة التلاعب في معطيات نظام المعالجة الآلية للمعطيات، أو جريمة الاعتداء على المعطيات خارج النظام...والتي سنتناولها لاحقا بالتفصيل.

وكمثال على الركن المادي لجريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، ما نصت عليه المادة (394مكرر) من (ق.ع.ج): "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة مالية من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طرق

---

[1] حنان ريحان مبارك المضحكي، المرجع السابق، ص87.

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي، المرجع السابق، ص ص113-114.

[3] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات-دراسة مقارنة، دار الفكر الجامعي، الإسكندرية مصر ،2013، ص ص46-47.

الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى (2) سنتين و الغرامة من 500.000 دج إلى 150.000 دج".

يتمثل الركن المادي لهذه الجريمة في صورتين: الأولى الصورة البسيطة تتلخص في مجرد الدخول أو البقاء غير المشروع فيما الصورة الثانية المشددة، تتحقق بتوافر الظرف المشدد لها ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع، إما محو أو تغيير في المعطيات الموجودة في النظام، أو تخريب لنظام اشتغال المنظومة ونقصد بفعل الدخول، الولوج إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات. ولم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة، ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر، أما فعل البقاء فهو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام[1].

وعليه يتحقق الركن المادي في هذه الجريمة بدخول المجرم المعلوماتي إلى نظام المعالجة الآلية للمعطيات بطريق الغش أو بالبقاء فيه أو في جزء منه، إما أنه ليس من بين المشتركين أو أنه غير مرخص له بالدخول، أو له الحق في الدخول إلا أنه بقي في النظام بعد انتهاء المدة المصرح له بها[2].

الفرع الثاني: الركن المعنوي:

لم يعرف المشرع الجزائري القصد الجنائي على غرار غالبية التشريعات واكتفى بالنص في الجرائم على العمد. كما لا يكفي لقيام الجريمة ارتكاب عمل مادي فقط، بل لا بد من أن يصدر أيضا عن إرادة الجاني. هذه العلاقة التي تربط العمل المادي بالفاعل تسمى بالركن المعنوي، الذي يتمثل في نية داخلية يضمرها الجاني في نفسه، ومن ثمة يتخذ الركن المعنوي صورتين أساسيتين هما: صورة الخطأ العمد أي: القصد الجنائي، وصورة الخطأ غير العمد أي: الإهمال وعدم الاحتياط[3]. إن الركن المعنوي في مختلف الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات تتخذ صورة القصد الجنائي إضافة إلى نية الغش، فالجرائم الإلكترونية هي من جرائم التقنية العالية تتطلب من المجرم الإلكتروني قدرا من المعرفة والتخصص، فكان من المتصوّر غالبا وقوعها في صورة واحدة هي صورة

---

1 علي عبد القادر القهوجي، المرجع السابق، ص ص120-122.

2 جميل عبد الباقي الصغير، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، مصر، ط1، 1992، ص150.

3 أحسن بوسقيعة، الوجيز في القانون الجنائي العام، المرجع السابق، ص121.

العمد، على اعتبار أن الجاني خطط ودبّر لارتكاب جريمته من أجل الحصول على المعلومات أو لاختراق شبكة الحاسوب، أو الاعتداء على أنظمة المعالجة الآلية للمعطيات سواء بالإدخال أو المحو أو التعديل[1].

فمثلا جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، هي جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة[2]، فيلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء بهدف الإدخال أو المحو أو التعديل، وأن يعلم بأن سلوكه هذا يؤدي للتلاعب في المعطيات، كما يجب أن يعلم أنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاؤه داخل النظام مشروعا، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء، أو كان يجهل بوجود حظر للدخول أو البقاء[3].

تجدر الإشارة إلى أننا سنتطرق بالتفصيل إلى الركن المادي والركن المعنوي لكل جريمة من الجرائم الإلكترونية التي نص عليها المشرع الجزائري بموجب القانون العام أو ضمن قوانين خاصة وهذا في فحوى الفصل الثاني من هذا الباب.

المطلب الثالث: الشروع والاتفاق الجنائي في الجريمة الإلكترونية

يتطلب مبدأ العقاب وقوع الجريمة، فهي تمثل عدوانا على المصالح محل الحماية القانونية ونظرا للطبيعة الخاصة للجريمة الإلكترونية وما تثيره من إشكالات في هذه البيئة الافتراضية، إرتينا أن نوضّح أولا مسألة الشروع في الجريمة الإلكترونية، وموقف المشرع الجزائري منه في (الفرع الأول)، ثم نتطرق ثانيا الى موضوع الاتفاق الجنائي في الجريمة الإلكترونية وموقف المشرع الجزائري في (الفرع الثاني).

الفرع الأول: مفهوم الشروع في الجرائم الإلكترونية، وموقف المشرع الجزائري منه:

سنتطرق أولا الى مفهوم الشروع، وثانيا إلى موقف المشرع الجزائري منه.

أولا: مفهوم الشروع: إذا كان الهدف من العقاب على الجرائم بمختلف أنواعها وخاصة الجرائم الإلكترونية المستحدثة، هو تعديها على المصالح التي يحميها القانون، فإن العلّة من العقاب على

---

[1] نبيلة هبة هروال، المرجع السابق، ص50.

[2] تجدر الإشارة إلى أن القضاء الأمريكي لم يستقر على حال، بخصوص ما إذا كانت تتطلب بعض الجرائم الإلكترونية قصدا عاما أم خاصا، كما هو الحال في جريمة التهديد عبر البريد الإلكتروني، إذ يكتفي بالقصد العام فقط، راجع، نبيلة هبة هروال، المرجع نفسه ص50.

[3] علي عبد القادر القهوجي، المرجع السابق، ص 134، راجع أيضا، فايز الظفيري، المقال السابق، ص ص520-521.

الشروع بوصفه جريمة هو وجود خطر يهدد هذه المصالح، فهو بمثابة اعتداء محتمل فالمشرع لا يحمي المصالح القانونية من الضرر الذي يلحقها فقط، وإنما يوفر لها حماية إزاء الخطر الذي يهدد باحتمال القضاء عليها[1]. إذا كانت الجريمة لا تكتمل إلا بتوافر ركن مادي، فإنه ليس من الضروري أن يترتب على هذا الفعل نتيجة ضارة حتى يعاقب عليها، فإذا تحققت النتيجة نكون بصدد الجريمة التامة، وإذا لم تتحقق نكون بصد الشروع[2]. عادة تمر الجريمة قبل تمامها بعدة مراحل منها ما هو مؤثم قانونا وتمتد إليه يد العقاب، ومنها ما هو غير مؤثم ويفلت من العقاب، وهذه المراحل هي مرحلة التفكير في الجريمة، ومرحلة التحضير للجريمة، ومرحلة البدء في التنفيذ[3].

تتعلق المرحلة الأولى بالجانب النفسي إذ تكون الجريمة عبارة عن فكرة محضة لا عقاب عليها إلا إذا نص القانون على خلاف ذلك مثل: نص المادة (176) من (ق.ع.ج) التي عاقبت على مجرد التصميم المشترك بخصوص تكوين جمعيات الأشرار وهو ما يتعلق بالاتفاق الجنائي، أما المرحلة الثانية فتتعلق بالأعمال التحضيرية التي تتوسط التفكير في الجريمة والبدء في التنفيذ، وهي تتخذ جانبا ماديا يقتضي من الجاني مباشرة أعمال استعدادا للتنفيذ، فهي تختلف عن مرحلة التفكير من كونه سلوكا ماديا خارجيا. كما تختلف عن مرحلة الشروع من حيث كونه سابقا عن البدء في تنفيذ الجريمة، فهو بمثابة ممهد للبدء في التنفيذ، ويعتبر من قبيل الأعمال التحضيرية شراء مادة سامة للقتل أو شراء أسلحة[4]. هذه المرحلة غير معاقب عليها إذ ترك المشرع فرصة للجاني للعدول عن جريمته، لكن إذا ارتقت هذه الأفعال إلى درجة الخطورة التي تمس المصالح المحمية، اعتبرها المشرع جريمة مستقلة بذاتها، ومثال ذلك نص المادة (394مكرر2) التي اعتبرت بعض الأفعال التحضيرية كالبحث والتصميم جريمة مستقلة، كذلك نص المادة (394مكرر5) التي تعاقب على الأعمال التحضيرية في صورة الاتفاق الجنائي. وأخيرا تأتي مرحلة الشروع التي تنصرف فيها إرادة الجاني إلى تنفيذ الجريمة فعلا، فيبدأ في تنفيذ الركن المادي غير أن الجريمة لا تتم لأسباب لا دخل لإرادة الجاني فيها، وهي مرحلة معاقب عليها قانونا.

ثانيا: موقف المشرع الجزائري من الشروع في الجرائم الإلكترونية: بالنسبة للمشرع الجزائري نص على الشروع (المحاولة) في المادة (30) من قانون العقوبات: "كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة الى ارتكابها تعتبر كالجناية نفسها إذا

---

[1] عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، ج1، ديوان المطبوعات الجامعية، الجزائر، ط6، 2005، ص164.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، المرجع السابق، ص107.

[3] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا–دراسة مقارنة، دار النهضة العربية، القاهرة مصر، 2010، ص1003.

[4] أحمد حسام طه تمام، المرجع السابق، ص594.

لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولولم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها"، غير أن المشرع لا يعاقب على الشروع في مواد الجنح إلا بنص ولا يعاقب إطلاقا على الشروع في مواد المخالفات، إذ تنص المادة (31) من (ق.ع.ج) على:" المحاولة في الجنحة لا يعاقب عليها إلا بناء على نص صريح في القانون والمحاولة في المخالفة لا يعاقب عليها إطلاقا."

أما بخصوص الجرائم الإلكترونية ونظرا لخطورة هذا النوع المستحدث من الجرائم وبوصفها جنحا، لم يخرج المشرع الجزائري في رسم سياسته الجنائية في هذا المجال عن نظام العقاب الذي رسمته القوانين والاتفاقيات الدولية[1]، مثل نص المادة (11) من (إ.أ.م.إ.م)[2] التي تجرم المحاولة وأيضا بموجب نص المادة (19) المتعلقة بالاشتراك والشروع ضمن الفصل الثاني المتعلق بالتجريم من (إ.ع.م.ج.ت.م)، والتي تنص على:" ...الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية...". نص المشرع الجزائري في المادة (394مكرر7) من القسم السابع مكرر (ق.ع.ج) بعنوان: "المساس بأنظمة المعالجة الآلية للمعطيات" على:" يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

يظهر لنا من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال التي تضم الجرائم الماسة بنظام المعالجة الآلية للمعطيات نظرا لخطورتها، فعاقب على الشروع بنفس عقوبة الجريمة التامة، وهو مسلك محمود في سياسته الجنائية الرامية لمواجهة هذه الجرائم المستحدثة وسد كافة المنافذ أمام المجرم الإلكتروني. لكن بالمقابل هل عاقب المشرع الجزائري على الاتفاق الجنائي في الجرائم الإلكترونية؟. هذا ما سنتطرق إليه فيما يأتي:

---

[1] زيدان زيبحة، المرجع السابق، ص107.

[2] ***Article 11 – Tentative et complicité***

1." Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des Articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des Articles 3 à 5, 7, 8, 9 (1)a et 9(1)c de la présente Convention. ", convention européenne de la cybercriminalité, Op.Cit,p.6.

الفرع الثاني: مفهوم الاتفاق الجنائي في الجرائم الإلكترونية، وموقف المشرع الجزائري منه:

سنتناول أولا مفهوم الاتفاق الجنائي وأركانه، ثم نتطرق ثانيا إلى موقف المشرع الجزائري منه بخصوص هذا النوع المستحدث من الجرائم.

أولا: مفهوم الاتفاق الجنائي وأركانه: لم يعط المشرع الجزائري تعريفا للاتفاق أو الجمعية، إلا أنه لاكتساب الصفة الجرمية لهذا الفعل يجب انعقاد إرادتين أو أكثر للقيام بذلك و"الجمعية والاتفاق عبارتان تفيدان المعنى نفسه تقريبا ولكن الجمعية أكثر هيكلة من الاتفاق الذي يغلب عليه الطابع الفكري"[1]، فنصت المادة (176) من (ق.ع.ج) على:" كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه تشكل أو تؤلف بغرض الإعداد لجناية أو أكثر، أو لجنحة أو أكثر، معاقب عليها بخمس (5) سنوات حبس على الأقل، ضد الأشخاص أو الأملاك تكون جمعية أشرار، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل".

رغم أهمية تجريم هذا السلوك إلا انه أثار جدليا فقهيا، حيث يرى بعض من الفقه أن الاتفاق الجنائي، وإن كان للجاني عزم إجرامي، فإن المعاقبة عليه لا يعد استثناء على قاعدة عدم العقاب على مجرد العزم على ارتكاب الجريمة، بسبب أن المشرع لا يعاقب على الاتفاق الجنائي كخطوة للجريمة، وإنما يعاقب عليه في حد ذاته كجريمة مستقلة. في حين يرى جانب آخر من الفقه أن هذه الحجج غير سديدة، فحينما نقارن بين خطورة الاتفاق الجنائي وخطورة الأعمال التحضيرية التي يسعى فيها المجرم للقيام بفعله بمفرده، فالاتفاق الجنائي يعتبر مرحلة نفسية مبكرة للتحضير للجريمة، فكان الأولى على المشرع تجريم مرحلة الأعمال التحضيرية التي يقوم فيها المجرم فعلا ببعض الأفعال التحضيرية تمهيدا لارتكاب جريمته[2].

بالمقابل تفادى المشرع الجزائري هذا النقد، ولم يجرم مجرد العزم كما فعل في نص المادة (176) سالفة الذكر حيث يكتفي المشرع بمجرد التصميم المشترك على القيام بالفعل ، بل اشترط في هذا النوع من الجرائم أن يكون مجسدا بفعل أو عدة أفعال مادية طبقا لنص المادة(394مكرر5) التي تنص على:" كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها ".

---

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، المرجع السابق، ص480.

[2] رشيدة بوكر، المرجع السابق، ص ص341-342.

يمكن استخلاص أركان الاتفاق الجنائي من نص المادة (394مكرر5) من (ق.ع.ج) كما يأتي:

أ- **تعدد الجناة:** يتم الاتفاق بين شخصين على الأقل، أي توافر إرادتين، كما أنه لا يرد قيد على الحد الأقصى بموجب نص المادة (394مكرر5) التي تنص على:"...كل من شارك في مجموعة أو اتفاق..."، والأمر نفسه نصت عليه المادة (176) " كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه..." فإذا ارتكب الشخص العمل التحضيري المادي شخص واحد بمفرده أو بمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر، كما يجب أن تتجه هذه الإرادات إلى جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، وعليه لا يعاقب استنادا لهذا النص الاتفاق بهدف ارتكاب جنحة تقليد البرامج المعاقب عليها بموجب نصوص حق المؤلف والحقوق المجاورة[1].

ب- **موضوع الاتفاق الجنائي:** إذا لم يكن للاتفاق صفة جرمية وكان مشروعا لا عقاب عليه غير أن المشرع حدد الصفة الجرمية حينما حصرها في الإعداد بأفعال مادية للجرائم الماسة بالمعالجة الآلية للمعطيات بموجب نص المادة (394مكرر5) سالفة الذكر، كما لا يعني هذا ضرورة الإعداد لكافة الجرائم المشمولة بهذا القسم، بل يكفي الإعداد والتحضير لواحدة فقط، وهو ما يستفاد من نص المادة سالفة الذكر التي تنص على:"...لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم..." .يكفي أن يتم التحضير بفعل مادي مثل: تبادل المعلومات الهامة لارتكاب الجريمة كالإعلان على كلمة مرور *(mots de passe)* أو رمز الدخول *(code d'accès)*[2].

ج-**المشاركة في الاتفاق:** لم يكتف المشرع الجزائري بتجريم الاتفاق، بل تعداه لتجريم فعل الاشتراك في مجموعة أو في اتفاق بهدف الإعداد لجريمة من الجرائم الماسة بأنظمة لمعالجة الآلية للمعطيات، وحسنا فعل بسبب أن هذه الجرائم تتم عادة في إطار مجموعات، وتحسبا لسهولة الاتفاق وسرعته بين المجرمين في هذا المجال حتى وإن لم يكن بينهم معرفة مسبقة أو اتصال مباشر[3]، كما وسّع المشرع من نطاق العقوبة حينما أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي، وذلك بهدف ردع مجرمي هذا النوع المستحدث من الجرائم، وبمفهوم المخالفة تعتبر الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بهذا النص[4].

---

[1] رشيدة بوكر، المرجع السابق، 345.

[2] آمال قارة، المرجع السابق، ص ص131-132.

[3] زيدان زيبحة، المرجع السابق، ص105.

[4] آمال قارة، المرجع السابق، ص132.

د-القصد الجنائي: تقوم جريمة الاتفاق الجنائي على العلم والارادة.

- **العلم:** يجب على كل عضو منضم للاتفاق الجنائي أن يعلم بماهية الفعل موضوع الاتفاق وعلى هذا الأساس فمن يجهل الغرض من الاتفاق، وهو ارتكاب جنح المساس بأنظمة المعالجة الآلية للمعطيات لا يعد القصد الجرمي متوافرا لديه .

- **الإرادة:** لا يكفي مجرد العلم بفحوى الاتفاق الجنائي، بل لا بد من توافر الإرادة الجادة لشخصين على الأقل للدخول أو الاشتراك فيه، بمعنى أن تتضح إرادة كل واحد أن يكون طرفا في هذا الاتفاق، وأن يقوم بالدور الذي سيعهد إليه. فإذا لم تكن الإرادة على هذا النحو كأن تكون لمجرد الاستطلاع أو للعبث، ينتفي عنه القصد الجرمي لانتفاء إرادته الجادة[1].

ثانيا: موقف المشرع الجزائري من الاتفاق الجنائي في الجرائم الإلكترونية: بناء على ما سبق ذكره، يمكن القول أن المشرع الجزائري جعل عقوبة الاتفاق الجنائي تتناسب وطبيعة الجرائم الواقعة على نظام المعالجة الآلية للمعطيات، على خلاف نص المادة (177) من قانون العقوبات التي حددت العقوبة على الاتفاق الجنائي العام على أساس خطورة الجريمة، حيث تنص على:" يعاقب على الاشتراك في جمعية الأشرار بالسجن المؤقت من خمس (5) سنوات إلى (10) عشر سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، إذا تم الإعداد لارتكاب جنايات. و تكون العقوبة الحبس من سنتين (2) إلى خمس (5) سنوات والغرامة من 100.000 دج إلى 500.000 دج، إذا تم الإعداد لارتكاب جنح. ويعاقب منظم جمعية الأشرار أو من يباشر فيها أية قيادة كانت بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 1.000.000 دج إلى 5.000.000 دج"، كما يلاحظ أن المشرع الجزائري تجاوب مع نصوص الاتفاقيات الدولية ومقررات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر وما تضمنه القرار الصادر عن مؤتمر الأمم المتحدة الثامن عشر لمنع الجريمة ومعاملة السجناء المتعلق بالجرائم ذات الصلة بالكمبيوتر، والتي خلصت في مجملها إلى تجريم الاتفاق الجنائي[2].

المطلب الرابع: تطور المنظومة القانونية لمكافحة الجرائم الإلكترونية في الجزائر

انطلقت عملية استغلال شبكة الإنترنت في الجزائر منذ سنة 1995، ومع إساءة استخدام هذه التقنية الحديثة، ظهرت جرائم مستحدثة تختلف تماما في مفهومها عن الجرائم التقليدية، مما دفع بالمشرع الجزائري إلى تعديل منظومته الجزائية للحد من انتشارها، وكان ذلك بداية من سنة2004

---

[1] على عبد القادر القهوجي، المرجع السابق، ص ص117-118.

[2] زيدان زيبحة، المرجع السابق، ص ص105-106.

سنتعرف أولا على جملة القوانين المتعلقة بمواجهة الجرائم الإلكترونية في(الفرع الاول)، ثم نعرج على مدى انتشار هذه النوع من الجرائم المستحدثة في الجزائر ضمن (الفرع الثاني).

الفرع الأول: القوانين المتعلقة بمواجهة الجرائم الإلكترونية:

مع التطور المذهل الحاصل في مجال الحوسبة والاتصال، سارعت الجزائر على غرار دول العالم لاستغلال هذه التقنية في شتى المجالات، عن طريق تسطير برامج طموحة مثل: ربط الجزائر بشبكة الإنترنت عالية التدفق عن طريق الأقمار الصناعية أو الكوابل، وتمكين مؤسسات الدولة من التعامل بهذه التقنية للوصول لحكومة إلكترونية رائدة، ناهيك عن إيصال الإنترنت لكل بيت وبتدفق عالي، إضافة إلى تمكين كل أسرة جزائرية من شراء حاسوب مثل: برنامج (أسرتيك)، كما تم فتح مجال استغلال الهاتف النقال للخواص...إلخ. فمن خلال هذه المعطيات لا شك أن هناك جرائم إلكترونية عديدة ترتكب سواء كان الحاسوب هدفا أو وسيلة لها، أو الجرائم التي ترتكب بواسطة شبكة الإنترنت، أو التي ترتكب باستعمال شبكات الاتصال، لذا سارع المشرع الجزائري إلى حماية هذا الفضاء السبراني ومستعمليه من خلال إصدار جملة من القوانين سواء ما تعلق بالقانون العام أو بموجب نصوص خاصة، أو ما تعلق بالتصديق على الاتفاقيات العربية والدولية، وهي تمثل بداية لمنظومة قانونية فعّالة ومتكاملة لمكافحة هذه الجرائم.

سنتعرف على معالمها حسب ترتيبها الزمني ودون تفصيل، لأنّنا سنتطرق إلى ذلك في الفصل الثاني من الباب الأول الذي يتناول الأحكام الموضوعية للجرائم الإلكترونية، حيث سنفصل في أركان كل جريمة على حدة، كما نتطرق أيضا بالتفصيل إلى الجوانب الإجرائية في الفصل الأول من الباب الثاني .

أولا: بخصوص تعديل قانون العقوبات: في طار مكافحة الجرائم الإلكترونية التي تعتبر ذات طبيعة خاصة، قام المشرع الجزائري بتعديل قانون العقوبات على مراحل، نوجزها كما يلي:

1- القانون رقم: 01-09 المؤرخ في:2001/06/26: نظرا لانتشار الوسائل الإلكترونية والمعلوماتية وتوسع شبكة الإنترنت، قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم:01-09 المعدل والمتمم لقانون العقوبات في القسم الأول تحت عنوان: "الإهانة والتعدي على الموظفين ومؤسسات الدولة[1]، فنص في المواد من(144 مكرر - 144 مكرر2) و المادة(146) على جرائم الإهانة والسب والقذف ضد رئيس الجمهورية ومؤسسات الدولة باستعمال الوسائل

---

[1] القانون رقم: 01-09 المؤرخ في: 2001/06/26 يعدل ويتمم الأمر رقم: 66-156 المؤرخ في: 1966/06/08، والمتضمن قانون العقوبات، (ج.ر) رقم:34 المؤرخة في:2001/06/27، ص ص5-18.

الإلكترونية أو المعلوماتية، حيث كان هدف المشرع منع المجرم الإلكتروني من إساءة استخدام هذا الفضاء الافتراضي، وتمهيد الطريق نحو توسيع مكافحة هذا النوع من الجرائم المستحدثة إلى مجالات أخرى كما سنرى.

2-القانون رقم: 04-15المؤرخ في: 10-11-2004: كما رأينا سلفا، ومع تقدم الجزائر في استغلال مجال تكنولوجيات الإعلام والاتصال، قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم: 04-15 سالف الذكر بإضافة قسم سابع مكرر تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات" من المادة (394 مكرر- 394 مكرر7)، بهدف مكافحة الجرائم المستحدثة الناشئة عن إساءة استعمال هذه التقنية. حيث نص على جملة من الجرائم كجريمة الدخول عن طريق الغش في كل أو جزء من منظومة معلوماتية، وجريمة تخريب نظام اشتغال المنظومة المعلوماتية...إلخ-سنتطرق إلى هذه الجرائم بالتفصيل في الفصل الثاني الخاص بالأحكام الموضوعية للجرائم الإلكترونية- وبالتالي نستطيع القول بأن المشرع الجزائري تدارك ولو نسبيا الفراغ القانوني في مجال مواجهة الإجرام الإلكتروني. وهي تمثل قفزة نوعية برغم أن دولا مجاورة سبقتنا في وضع قوانين في ذات الشأن مثل تونس(قانون العقد الإلكتروني لسنة2001) والمغرب(القانون رقم: 03-07 المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات)، كما تجدر الإشارة إلى أن المشرع الجزائري قد ركز في هذا القانون على الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، وأغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي والمتمثلة في التزوير المعلوماتي.

3- قانون رقم:06-23 المؤرخ في:2006/12/20: مع التزايد الكبير في استعمال تقنية المعلومات، وللأسباب السابق ذكرها، ونظرا لخطورة الأفعال الواقعة على الحياة الخاصة للأفراد، وسّع المشرع الجزائري تدريجيا من سياسته الجنائية الخاصة بالتجريم والعقاب إلى جرائم المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت، كاستعمال الحاسوب وشبكة الإنترنت، والهاتف النقّال...إلخ، وهذا بموجب القانون رقم: 06-23 المعدل والمتمم لقانون العقوبات، أين نصت المواد من(303 مكرر - 303 مكرر3)[1] على: التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه، أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

4- القانون رقم:09-01 المؤرخ في:2009/02/25: نظرا للإشكالات الفقهية التي أثيرت حول مدى اعتبار المعلوماتية مالا، سارع المشرع الجزائري إلى اعتبار المعلوماتية مالا يمكن سرقته

---

[1] القانون رقم:06-23 المؤرخ في:2006/12/20 يعدل ويتمم الأمر رقم: 66-156 المؤرخ في: 1966/06/08، والمتضمن قانون العقوبات، (ج. ر) رقم:84 المؤرخة في:2006/12/24، ص ص11-29.

وذلك بموجب القانون رقم: 09-01 المعدل والمتمم لقانون العقوبات[1]، أين نصت المادة (350مكرر1) من (ق.ع.ج) على: " يعاقب بالحبس من سنتين (2)إلى عشر (10) سنوات وبغرامة من 200.000 دج إلى 1.000.000 دج كل من سرق أو حاول سرقة ممتلك ثقافي منقول محمي أو معرف" ، وحسنا فعل المشرع نظرا لما يشكله المال المعلوماتي من قيمة مالية مستحدثة.

ثانيا: بخصوص تعديل قانون الإجراءات الجزائية: في إطار استكمال سياسته الجنائية الخاصة بمكافحة الجرائم الإلكترونية في شقها الإجرائي، كان لزاما على المشرع الجزائري تعديل قانون الإجراءات الجزائية بهدف استحداث إجراءات جديدة تتوافق والطبيعة الخاصة للجرائم الإلكترونية فنص القانون رقم:06-22 المؤرخ في:2006/12/20 يعدل ويتمم قانون الإجراءات الجزائية[2]، على جملة من الإجراءات الجديدة في الفصل الرابع تحت عنوان: "في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" من المادة (65 مكرر 5 – 65 مكرر10)، كما نص أيضا في الفصل الخامس تحت عنوان: "في التسرّب" بموجب المادة (65 مكرر11 – 65 مكرر18)، وهي إجراءات تمكن سلطات البحث والتحري من الكشف عن المجرم الإلكتروني في هذه البيئة الافتراضية التي يصعب التحقيق فيها بسبب طبيعتها الخاصة كما رأينا سلفا.

ثالثا: بخصوص القوانين الخاصة:

1- قانون رقم:2000-03 المؤرخ في: 2000/08/05 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السّلكية واللاّسلكية[3]: نص هذا القانون في جزء منه على الاستغلال الأمثل لتكنولوجيا تحويل الأموال بواسطة الطريق الإلكتروني، وهذا بموجب نص المادة (87)[4]، كما اعتبر المشرع المسؤولية قائمة على عاتق المتعامل فيما يخص المبالغ المحولة بموجب نص المادة (2/84)، ويمثل هذا المجال بيئة خصبة للمجرم الإلكتروني لارتكاب جرائم سرقة وتحويل الأموال...إلخ، لذا أضفى المشرع حماية جزائية على استغلال هذه التكنولوجيا نظرا لما ينجر عنها من

---

[1] القانون رقم:09-01 المؤرخ في:2009/02/25، يعدل ويتمم الأمر رقم: 66-156 المؤرخ في: 1966/06/08، والمتضمن قانون العقوبات، (ج. ر) رقم:15 المؤرخة في:2009/03/08، ص ص3-8.

[2] القانون رقم:06-22 المؤرخ في:2006/12/20، يعدل ويتمم الأمر رقم: 66-155 المؤرخ في: 1966/06/08، والمتضمن قانون الإجراءات الجزائية، (ج. ر) رقم:84 المؤرخة في:2006/12/24، ص ص4-10.

[3] القانون رقم :2000-03 المؤرخ في:2000/08/05، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السّلكية واللاّسلكية، (ج. ر) رقم:48 المؤرخة في:2000/08/06، ص ص3-26.

[4] تنص المادة (87) من القانون رقم: 2000-03 على: "يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق الإلكتروني".

أضرار تمس مصالح الدولة والأفراد على حد سواء، فأحاط سرية المراسلات التي هي حق دستوري مكفول بحماية خاصة بموجب نص المادتان (105) و(137) من القانون نفسه.

2- الأمر رقم:03-05 المؤرخ في: 2003/06/19 يتعلق بحقوق المؤلف والحقوق المجاورة: إن أهم ما جاء به هذا الأمر بخصوص مكافحة الجرائم الإلكترونية، هو تصنيف برامج الحاسوب بموجب المادة (04/أ) وقواعد البيانات بموجب المادة (1/05) . كما أحاطها بحماية جزائية تمثلت في جرائم التقليد، وهذا بموجب نصوص المواد من (143) وما بعدها، و(151) وما بعدها[1].

3- القانون رقم:08-01 المؤرخ في:2008/01/23 يتعلق بالتأمينات الاجتماعية: يمكن القول أن المشرع الجزائري في هذا القانون، قد استبق الأحداث تحسبا للتطور الهائل في مجال استعمال التكنولوجيا الحديثة، وتعميم استعمال الشبكة المعلوماتية في شتى المجالات، إذ نص في المادة (06مكرر) من هذا القانون على:" تثبت صفة المؤمن له اجتماعيا ببطاقة إلكترونية...". ونظرا لاحتواء هذه البطاقة على معلومات سرية تتعلق بالحياة الخاصة للأفراد، أحاطها بالحماية الجزائية اللاّزمة، فنص في المادة (93مكرر2) على:" دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين(2)إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 200.000 دج، كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمّن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة"، كما تضاعف العقوبة حسب نص المادة (93مكرر3) على كل من يقوم عن طريق الغش بتعديل أو حذف للمعطيات.

4- القانون رقم:09-04 المؤرخ في:2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: إن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، تطلب تدخلا تشريعيا صريحا سواء على المستوى الدولي أو الداخلي، حيث عرفت المادة (2/02) من القانون السالف الذكر، المنظومة المعلوماتية: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين". بدأت نصوص هذا القانون بتحديد المصطلحات ثم نصت على جملة من القواعد الإجرائية الجديدة الخاصة بحالات مراقبة الاتصالات الإلكترونية وبتفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية والتزامات مقدمي الخدمات، والتعاون والمساعدة القضائية الدولية، إضافة الى إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

---

[1] المادة (43) وما بعدها، والمادة (151) وما بعدها من الأمر رقم:03-05 يتعلق بحقوق المؤلف والحقوق المجاورة.

5- القانون رقم:15-04 المؤرخ في:2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[1]: تبعا لمتطلبات المعاملات الإلكترونية لاسيما في ظل التوجه نحو الحكومة الإلكترونية ومقتضيات التجارة الإلكترونية، وبعد أن أدرج المشرع الجزائري نظام الإثبات بالكتابة في الشكل الإلكتروني ضمن قواعد الإثبات. أقر بنظام التوقيع والتصديق الإلكترونيين والاعتراف بحجتيهما في الاثبات، قصد توفير الحماية اللاّزمة لوسائل الدفع الإلكتروني بالنسبة لمعاملات التجارة الإلكترونية وزرع الثقة لدى المتعاملين لما يمتاز به من مستوى عال للسرّية والخصوصية.

رابعا: الاتفاقيات العربية: وتشمل ما يأتي:

1- الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية: حررت بالقاهرة بتاريخ:2010/12/21 ، وصادقت عليها الجزائر بتاريخ: 2014/09/08، حيث تنص المادة (21) منها على:" تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي لتجريم ارتكاب أو المشاركة في ارتكاب الأفعال الآتية التي تقوم بها جماعة إجرامية منظمة في نطاق الاستعمال غير المشروع لتقنية أنظمة المعلومات :

- الاختراق غير المشروع أو تسهيل الاختراق غير المشروع على نحو كلي أو جزئي لأحد نظم المعلومات - تعطيل أو تحريف تشغيل أحد نظم المعلومات - إدخال بيانات بطرق غير مشروعة في أحد نظم المعلومات أو مسح أو تعديل أو نسخ أو نشر البيانات التي يحتويها هذا النظام بطريق غير مشروع-استيراد أو حيازة أو عرض أو ترك أو إتاحة إحدى المعدات أو الأدوات أو برامج تقنية المعلومات بدون سبب مشروع بهدف ارتكاب إحدى الجرائم المنصوص عليها في الفقرات الثلاث السابقة -أي جريمة من الجرائم التقليدية ترتكب بإحدى وسائل تقنية أنظمة المعلومات.

2- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: حررت هذه الاتفاقية الهامة بالقاهرة في:21 ديسمبر2010، صادقت عليها الجزائر بالمرسوم الرئاسي رقم:14-252 المؤرخ في:2014/09/08. وهي تتويج لجهود الدول العربية في التصدي لهذا النوع المستحدث من الجرائم أكدت في مقدمتها على أنها جاءت رغبة من هذه الدول لتعزيز التعاون فيما بينها قصد مكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، ولتبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد هذه الجرائم، وأخذا بالمبادئ الدينية والأخلاقية السامية، ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم

---

[1] القانون رقم:15-04 المؤرخ في:2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، (ج. ر) رقم:06 المؤرخة في:2015/02/10، ص ص6-16.

ومع مراعاة النظام العام لكل دولة، حيث حددت المادة الأولى الهدف من الاتفاقية:" تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها". احتوت الاتفاقية على خمسة فصول بمجموع إثنان وأربعون مادة، شملت التعريف بالمصطلحات والنص على جرائم متعددة كجريمة التزوير وجريمة الاحتيال، وجريمة الإباحية وجرائم الاعتداء على حرمة الحياة الخاصة، وإجراء التفتيش والتعاون القانوني والقضائي وتسليم المجرمين...إلخ.

تعتبر هذه الاتفاقية نقطة تحول هامة، فحسنا فعل المشرع الجزائري حينما صادق عليها، لأنها جاءت مدعمة لسياسته الجنائية السابقة وتكملة للنقائص المسجلة فيها، خاصة ما تعلق ببعض الجرائم مثل: التزوير المعلوماتي والإباحية الإلكترونية...إلخ، وننتظر من المشرع تحويل هذه الاتفاقية الى نصوص قانونية خاصة بمكافحة الجرائم الإلكترونية.

خامسا: بعض الاتفاقيات الدولية: نذكر منها:

1- اتفاقية حماية حقوق المؤلف بباريس بتاريخ:1971/07/24، انضمت إليها الجزائر بموجب المرسوم الرئاسي رقم:71-741 المؤرخ في:1971/09/18.

2- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من طرف الجمعية العامة بتاريخ:2001/05/31، صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم:04-165 المؤرخ في:2004/06/08.

3- اتفاق الشراكة الأورو متوسطي بين الاتحاد الأوروبي والجزائر بتاريخ:2002/04/22 صادقت عليه الجزائر بموجب القانون رقم:1144/2003 بتاريخ:2003/12/02.

4- إبرام اتفاقية دولية ثنائية مع الحكومة الفرنسية والمتعلقة بـ: "التعاون في مجال الأمن ومكافحة الإجرام المنظم"، حيث تنص المادة (10/01) من الاتفاقية على:"...مكافحة الاحتيالات المرتبطة بتكنولوجيات الإعلام والاتصال الجديدة..."[1].

الفرع الثاني: انتشار الجرائم الإلكترونية في الجزائر:

على غرار دول العالم المتقدمة، اهتمت الجزائر منذ تسعينيات القرن الماضي باستغلال التكنولوجيا الحديثة في مجال تكنولوجيات الإعلام والاتصال في شتى الميادين، وعرفت نموا متسارعا في عدد المبحرين على شبكة الإنترنت، ويتم تجهيز المنازل الجزائرية أكثر فأكثر بأجهزة إلكترونية

---

[1] المرسوم الرئاسي رقم:07-375 المؤرخ في:2007/12/01 المتعلق بالتعاون في مجال الأمن ومكافحة الإجرام المنظّم، (ج. ر) رقم:77 المؤرخة في:2007/12/09، ص6.

خاصة كالحواسيب المنزلية والشخصية وربطها بشبكة الإنترنت *(ADSL)*. بل تعدى ذلك إلى استعمال تقنيات الجيل الثالث*(3G)* والرابع *(4G)*، حيث أدرك الجميع أهمية استغلال تكنولوجيا الإعلام والاتصال في عالم أصبح كالقرية لا يعترف فيه بالحدود الجغرافية.

ففي حصيلة قدمتها شركة اتصالات الجزائر للفترة الممتدة من 2003 إلى 2013[1] ، تبين فيها مدى تطور وانتشار شبكة الإنترنت والهاتف النقال، نتيجة عدة عمليات تحسين وتطوير وتنظيم قامت بها الدولة من أجل تطوير وتوسيع شبكات الاتصالات الوطنية والدولية. وهذا ما سمح بتوصيل المنازل والشركات ومقاهي الإنترنت *(Cybercafé)* بهذه الخدمة، حيث ارتفعت نسبة توفر الإنترنت ذو التدفق السريع في المنازل من 1 % في سنة 2005 إلى 20 % في سنة 2013. أما فيما يتعلق بعدد أجهزة الإنترنت ذو التدفق السريع، فلقد انتقلت من 56.000 في 2005 إلى 1.309.454 في نهاية شهر مارس 2013. من جانب آخر وفيما يتعلق بعدد مشتركي شبكة الإنترنت ذو التدفق السريع فلقد انتقل من 178.707 زبون في نهاية 2007 إلى 1.188.201 في مارس 2013 حيث 60 % منهم يستفيد من خدمة الإنترنت ذو التدفق السريع مع مودم *(WIFI)*. وفي الصدد نفسه ورد في تقرير محاضرة الأمم المتحدة حول التجارة والتطور (تقرير الإعلام الاقتصادي لسنة 2009 الاتجاهات والتوقعات)، أنه تم تصنيف الجزائر من بين الدول الإفريقية الخمسة التي تجمع 90 % من مشتركي الإنترنت ذو التدفق السريع إلى جانب المغرب وتونس ومصر وجنوب إفريقيا.

أما بخصوص عدد مشتركي الهاتف النقال، أشار التقرير الصادر عن الاتحاد الدولي للاتصالات *(UIT)* لسنة2013، أن عدد المشتركين في خدمات الهاتف النقال في الجزائر، بلغ حوالي 39.69 مليون مشترك، يتقاسم هذا العدد ثلاثة متعاملين هم نجمة، موبيليس وجيزي[2]. كما نشرت دراسة أجريت سنة 2009 حول توجهات مستعملي شبكة الإنترنت في الجزائر[3] أن عدد المبحرين على شبكة الإنترنت يقدر بحوالي 4.5 مليون أي بمعدل 12% من عدد السكان، يمثل الرجال منهم 74.2% وتمثل النساء 25.8 %، وأن 6 مبحرين من أصل 10 سنّهم أقل من 40 سنة، أما بخصوص مجالات الاستعمال، وضحت الدراسة الآتي:

---

[1] التقرير موجود على الموقع الرسمي لاتصالات الجزائر على الرابط الآتي:

http://www.algerietelecom.dz/AR/?p=at_histoire_realisations، تاريخ الاطلاع:2015/04/28، على الساعة:10:33

[2] التقرير منشور على الموقع الرسمي للاتحاد الدولي للاتصالات على الرابط الآتي:

http://telecomworld.itu.int/outcomes/2013-report/،تاريخ الاطلاع:2015/04/28 على الساعة:11:27.

[3] الدراسة منشورة على الرابط الآتي:*www.webdialna.com/pdf/presse.pdf*، تاريخ الاطلاع:2015/04/28على الساعة:11:06، ص ص1-7.

1- للاتصال والتواصل : 82.6% يرسلون ويستقبلون رسائل إلكترونية *(Email)*، و42,5% لبرامج المحادثة على شبكة الإنترنت مثل: *(MSN)،(Yahoo Messenger)*...إلخ و33,8% مسجلون أو يزورون المنتديات*(Forums)*، و33% تمثل إجراء مكالمات هاتفية عن طريق الإنترنت باستعمال برامج مثل: *(Skype)*، و9,9% من أجل المؤتمرات بالفيديو عن طريق الإنترنت (*vidéo conférence)*.

2- للبحث على المعلومات: 80,7% يستعملون محرك البحث*(Google)*، و 22,9% يرغبون في ربط علاقة تجارية...إلخ.

3- وسيلة للإعلام: 80,8% لقراءة الجرائد على الإنترنت، و19,9% الاستماع إلى القنوات الإذاعية على الإنترنت، و11,4% يشاهدون قنوات التلفزة على الإنترنت.

فبالنظر للمعطيات السابقة، وقياسا على الانتشار والاستعمال الواسع لهذه التقنية، لا شك أنها تمثل بيئة خصبة للإجرام الإلكتروني على اختلاف أنواعه، سواء أكان الحاسوب أداة للجريمة أو هدف لها، أو جرائم ترتكب بواسطة شبكة الإنترنت أو بواسطة شبكات الاتصال.

بالنسبة للجزائر للأسف، ليست هناك إحصاءات رسمية حول الأضرار الناجمة عن الجرائم الإلكترونية، سواء كانت أضرار اقتصادية أو اجتماعية أو نفسية، وإنما هناك بعض الاحصائيات القليلة لعدد الجرائم الإلكترونية المرتكبة نوضحها في الجدول الآتي[1]:

---

[1] الإحصاءات موجودة على الموقع الرسمي للمديرية العامة للأمن الوطني على الرابط الآتي:
http://www.dgsn.dz/?%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A-%D9%8A%D8%B9%D8%A7%D9%84%D8%AC,4800 ، تاريخ الاطلاع:2016/10/09 على الساعة:09:50.

الرقم	نوع القضية	العدد	السنة	عدد الجناة	ملاحظة
01	جرائم إلكترونية.	12	2011	غير متوفر	لم تحدد
02	جرائم إلكترونية.	47	2012	غير متوفر	لم تحدد
03	الإحصاء غير متوفر لسنة 2013.				
	جريمة المساس بأنظمة المعالجة الآلية للمعطيات.	75			
	قضايا لها علاقة بالقذف وبالمساس بحرمة الحياة الخاصة.	59			
	التهديد بالتشهير باستعمال شبكة الإنترنت.	28			
	انتحال هوية الغير.	26			
	نشر الصور المخلة بالحياء.	09			
	النصب والاحتيال عن طريق الإنترنت.	03			
	الإهانة والسب عن طريق الإنترنت.	06			
	الاستعمال غير الشرعي للبطاقات الإلكترونية.	02			
	أعمال القرصنة(حجز 334515 قرص مضغوط مقلد.				

من خلال هذا الجدول، يمكن ملاحظة أن الجريمة الإلكترونية في الجزائر في ازدياد مستمر خاصة مع استمرار الدولة في توسيع شبكة الإنترنت وتحسين تدفقها، وتوفير خدمات جديدة مثل: تقنية *(G3)* و*(G4)* مما ضاعف من عدد المشتركين، ففي هذا الشأن أوضحت خريطة ثلاثية الأبعاد أعدتها شركة *(Kaspersky)* الرائدة في مجال أنظمة الحماية في مجال المعلوماتية، عن التهديدات

الإلكترونية المختلفة خلال الثلاثي الأول من سنة 2014، أن الجزائر جاءت في مقدمة الدول العربية المصابة ببرمجيات خبيثة أو تهديدات إلكترونية، وذلك بعد أن احتلت المرتبة الحادية عشرة عالميا مسجلة بذلك 18.3 مليون اختراق خلال الثلاثي الأول فقط من السنة نفسها. وتظهر الإحصاءات أن الجزائر لديها أعلى مستوى تهديدات قادمة من الشبكات المحلية، وعن طريق منافذ وأجهزة *(USB)* والأقراص المدمجة وأقراص الفيديو الرقمية، فيما تقدر نسبة التهديدات المحلية بـ 54.5 بالمائة و31.6 بالمائة التهديدات على الإنترنت. وأكّد التقرير أن أكثر المؤسسات تعرضا للهجمات هي المؤسسات الحكومية والمالية وحسابات المواطنين[1]. وبناء على هذا التقرير لا شك أن هناك أضرار مالية ضخمة تصيب مؤسسات الدولة والمواطنين على حد السواء بما يستلزم من المشرع وضع آليات قانونية رادعة للحد من انتشار هذه الجرائم المستحدثة، وهو ما سنتعرف عليه لاحقا.

---

[1] للاطلاع أكثر، يرجى زيارة الموقع الرسمي لشركة *(Kaspersky)* على الرابط الآتي: *https://cybermap.kaspersky.com* ، تاريخ الاطلاع: 2015/01/19: التوقيت: 09:21.

خلاصة الفصل الأول:

تطرقنا في هذا الفصل إلى تعريف الحاسوب وشبكة الإنترنت، كما اطلعنا على دور الحاسوب في ارتكاب الجريمة فقد يكون هو نفسه هدفا لها أو يكون وسيلة لارتكابها. كما تتعدد دوافع المجرم في ارتكاب الجرائم الإلكترونية، فقد تكون دوافع شخصية أو خارجية تكون نتيجتها إحداث أضرار بالغة على الفرد والمجتمع سواء كانت أضرارا اقتصادية أو نفسية أو اجتماعية.

من جانب آخر، لا يوجد اتفاق على المستوى التشريعي أو الفقهي على استعمال مصطلح محدد للدلالة على هذه الظاهرة الجرمية، وهذا بسبب طبيعتها الخاصة، فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود.

بالنسبة للمشرع الجزائري وُفق في اعتماد مصطلح "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال" وعرّفها بموجب أحكام المادة (02/أ) من القانون رقم: 04 – 09، للدلالة عليها، والذي يتوافق أيضا مع مصطلح "الجرائم الإلكترونية" بالمفهوم الموسع والذي استعملناه في بحثنا هذا. أما فيما يخص وضع تعريف لها فظهر اتجاهان فقهيان يمثل الأول المفهوم الضيق للجرائم الإلكترونية والثاني المفهوم الموسع لها، وهذا الأخير أخذ به المشرع الجزائري في وضع سياسته الجنائية لمكافحتها.

من جهة أخرى، اختلف الفقهاء أيضا عند محاولة وضع تصنيف لها، فتبين أنها ليست فئة واحدة، وبالتالي تعددت التصنيفات سواء ما تعلق بمحل الجريمة أو دور الكمبيوتر في ارتكابها، أو كجرائم ماسة بالأموال أو الأشخاص أو جرائم إنترنت. تطرقنا أيضا إلى الطبيعة القانونية الخاصة للجرائم الإلكترونية، فهي طبيعة من نوع خاص كون المعلومات هي محور ارتكاز هذا النمط من الجرائم. كما أنها تتميز بخصائص متفردة سواء ما تعلق بالجريمة نفسها، أو بالمجرم الإلكتروني كالذكاء والاحترافية، أو بأنواع المجنى عليهم، أو بمراحل ارتكابها، فهي جرائم عابرة للحدود ويصعب على المحققين اكتشافها وإثباتها، وتتم بأساليب وأدوات متنوعة يغلب عليها الطابع التقني، وهذا ما يميزها عن باقي الجرائم التقليدية.

كما تطرقنا أيضا إلى البنيان القانوني للجريمة الإلكترونية، حيث تناولنا أركانها إضافة إلى توضيح إشكالية مدى اعتبار المعلوماتية موضوعا لنصوص جرائم الأموال ومدى خضوعها أيضا لنصوص الملكية الصناعية والأدبية، وخلصنا إلى إضفاء المشرع الجزائري الحماية الجزائية على برامج الحاسوب وقواعد البيانات بموجب الأمر رقم:03-05 يتعلق بحقوق المؤلف والحقوق المجاورة وأحاطها بحماية جزائية بموجب جرائم التقليد، كما عاقب المشرع على الشروع والاتفاق الجنائي وبالتالي كان لزاما عليه عند وضعه لسياسته الجنائية، الإحاطة الشاملة والمعرفة الدقيقة بماهية هذه الجرائم المستحدثة وبكافة صورها، وتحديد أركانها وأوجه النشاط الجرمي فيها قصد تحقيق الفعالية في

مكافحتها وضمان عدم إفلات المجرم. كما تطرقنا في الأخير وبصفة موجزة إلى واقع الجرائم الإلكترونية في الجزائر وتطور المنظمة القانونية لمكافحتها عن طريق عرض جملة النصوص القانونية المتعلقة بذلك.

الفصل الثاني: الجوانب الموضوعية للجرائم الإلكترونية

عرفنا سلفا أن الجرائم الإلكترونية جرائم مستحدثة جاءت نتيجة سوء استخدام تكنولوجيات الإعلام والاتصال، حيث تخلف آثارا نفسية واجتماعية واقتصادية وأمنية بالغة الخطورة سواء على أفراد المجتمع أو على الدولة. وبعدما عرفنا ماهية الجرائم الإلكترونية وبنيانها القانوني، سنتطرق في هذا الفصل إلى مجمل النصوص القانونية المجرّمة لها، وذلك بالتطّرق بصورة موجزة للركن الشرعي والمادي والمعنوي والعقوبات المقرّرة لكل جريمة على حدة سواء بموجب قانون العقوبات(المبحث الأول)، أو بموجب قوانين خاصة في (المبحث الثاني). ثم نتناول الجرائم الإلكترونية التي جاءت بها (إ.ع.م.ج.ت.م)، والتي صادقت عليها الجزائر بتاريخ:2014/09/08، وذلك بقصد التعرف على جملة الجرائم الجديدة التي جاءت بها نُصوصها والتي لازال المشرع الجزائري لم يدرجها بعد ضمن قانون العقوبات، وذلك في(المبحث الثالث).

المبحث الأول: مكافحة الجرائم الإلكترونية بموجب قانون العقوبات

بعد أن وضّح المشرع الجزائري البنيان القانوني للجريمة الإلكترونية، وتحديد معالمها بوضوح قام بتعديل قانون العقوبات للنص على جملة من الجرائم الإلكترونية خاصة ما تعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات. كما أننا سنبين بصفة عامة دون تفصيل الركن الشرعي والمادي والمعنوي في كل جريمة على حدة إضافة إلى العقوبات المقررة لها. سنبدأ بجرائم الإهانة أو السب أو القذف باستعمال الوسائل الإلكترونية أو المعلوماتية في (المطلب الأول)، ثم نتحدث عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ومدى كفاية النصوص المجرمة لكافة أشكال الاعتداء عليها في (المطلب الثاني)، كما نتطرق أيضا إلى جرائم الإرهاب الإلكتروني الذي أصبح يشكل هاجسا كبيرا للدول والحكومات في (المطلب الثالث)، لنختم في الأخير بجرائم المساس بحرمة الحياة الخاصة للأفراد باستعمال الوسائل التقنية، والتي باتت تشكل تهديدا كبيرا للخصوصية، وذلك في (المطلب الرابع).

المطلب الأول: جريمة الإهانة أو السب أو القذف باستعمال الوسائل الإلكترونية

تعتبر جرائم الذم والقدح والتحقير من أكثر الجرائم شيوعا في العالم الافتراضي، فالبعد الجغرافي بين الجاني والمجني عليه والمجهولية وسرعة انتشار الكلام الجارح عبر التقنية الرقمية، تساعد كلها على النيل من شرف وكرامة الإنسان، إذ تتم باستعمال شبكة الإنترنت(المجموعات الإخبارية المدونات، مواقع التواصل الاجتماعي، البريد الإلكتروني) أو باستعمال شبكة الهواتف النقالة...إلخ[1].

[1] عادل عزام سقف الحيط، المرجع السابق، ص198.

سنتطرق إلى جريمة الإساءة في حق رئيس الجمهورية في (الفرع الأول)، ثم نتطرق إلى جريمة السب أو القذف في حق مؤسسات الدولة في (الفرع الثاني).

الفرع الأول: جريمة الإساءة في حق رئيس الجمهورية:

تنطوي هذه الجريمة على جرائم الإهانة والقذف والسب باستعمال الوسائل الإلكترونية أو المعلوماتية، وسنتطرق إلى أركان كل جريمة على حدة.

أولا: جريمة الإهانة:

أ- **الركن الشرعي:** وهو الفعل المنصوص والمعاقب عليه في المادة (144)[1]من (ق.ع.ج) ونتيجة للتطورات المتلاحقة في تقنية المعلومات والاتصال، وما يمكن أن ينتج عنها من جرائم، قام المشرع بتعديل قانون العقوبات لمكافحة هذه الجريمة التي تتم في حق رئيس الجمهورية حماية لشخصه، والتي تتم باستعمال الوسائل الإلكترونية والمعلوماتية وهذا بموجب المادة (07) من القانون رقم:01-09 المؤرخ في:2001/06/26 يعدل ويتمم قانون العقوبات، حيث تنص المادة (144مكرر) على:" يعاقب بالحبس من (3) أشهر إلى اثني عشر(12) شهرا وبغرامة من 50.000 دج إلى 250.000دج أو بإحدى هاتين العقوبتين فقط كل من أساء لرئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأي آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى . تباشر النيابة العامة إجراءات المتابعة تلقائيا. في حالة العود، تضاعف عقوبة الحبس و الغرامة المنصوص عليها في هذه المادة".

ب- **مفهوم الإهانة:** لم يتطرق المشرع الجزائري لتعريف الإهانة، وبالرجوع للفقه هي:" كل قول أو فعل يحكم العرف بأن فيه ازدراء وطعن في الكرامة في أعين الناس، وإن لم يشمل قذفا أو سبا أو افتراء"[2].

---

[1] تنص المادة (144) من (ق.ع.ج) على:" يعاقب بالحبس من شهرين (2) إلى سنتين(2) وبغرامة من 1.000 دج إلى 500.000دج أو بإحدى هاتين العقوبتين فقط كل من أهان قاضيا أو موظفا أو ضابطا عموميا أو قائدا أو أحد رجال القوة العمومية بالقول أو الإشارة أو التهديد أو بإرسال أو تسليم أي شيء إليهم أو بالكتابة أو الرسم غير العلانيين أثناء تأدية وظائفهم أو بمناسبة تأديتها، وذلك بقصد المساس بشرفهم أو باعتبارهم أو بالاحترام الواجب سلطتهم. وتكون العقوبة الحبس من سنة إلى سنتين إذا كانت الإهانة الموجهة إلى قاض أو عضو محلف أو أكثر قد وقعت في جلسة محكمة أو مجلس قضائي. ويجوز للقضاء في جميع الحالات أن يأمر بأن ينشر الحكم ويعلق بالشروط التي حددت فيه على نفقة المحكوم عليه دون أن تتجاوز هذه المصاريف الحد الأقصى للغرامة المبينة أعلاه".

[2] العاقد غريب أحمد، جرائم الإهانة والقذف والسب، دراسة قانونية منشورة على الموقع الرسمي للنيابة الإدارية المصرية على الرابط الآتي:*http://ap.gov.eg/elmaktaba/Crimes%20of%20insult%20and%20defamation%20and%20insult.pdf*
تاريخ الاطلاع:2015/11/28، على الساعة:10:42، ص ص1-29.

ج–الركن المفترض: ويتعلق بصفة الضحية، وهو رئيس الجمهورية.

د–الركن المادي: يتمثل النشاط الجرمي في فعل الكتابة والرسم والتصريح، ففي الكتابة يمكن أن تكون في طريق عام يراها كل الناس، أو إذا عرضت للبيع في شكل معين، أو على صفحات مواقع الإنترنت...إلخ، أما الرسم أو الصورة يتسع مفهومها ليشمل على وجه الخصوص الرسوم الكاريكاتورية بأنواعها والصور المتحركة والأفلام السينمائية وكل التركيبات السمعية البصرية والتصريح، وكلها يتحقق فيها عنصر العلانية[1]. إن ما يهمنا هنا هو تبيان الوسائل الإلكترونية أو المعلوماتية المستعملة في ذلك، والتي ترك فيها المشرع الباب مفتوحا أمام ظهور وسائل إعلامية جديدة، هذه الوسائل تنطبق على جريمة الإهانة والسب والقذف. وعليه يقوم المجرم الإلكتروني بإساءة استخدام التقنية في المجال المعلوماتي والاتصال وشبكة الإنترنت، وسنوضح البعض منها كما يأتي:

- **شبكة الإنترنت:** يمكن لأي شخص يمتلك جهاز حاسوب متصل بشبكة الإنترنت من إنشاء موقع *(site)*[2]، يتضمن معلومات يمكن لأي شخص في العالم استقبال هذه المعلومات والاطلاع عليها، ويتم ارتكاب أفعال القدح والذم والقذف والسب خلال إسناد مادة كتابية أو سمعية أو سمعية بصرية من شأنها أن تنال من شرف الشخص وكرامته فتعرضه إلى بغض الناس واحتقارهم[3]، فمن خلال صفحات الإنترنت *(web pages)* يتم نشر وإذاعة وتوزيع هذه المحتويات ذات الطابع المعلوماتي[4]، وهو ما ينطبق أيضا على الجرائد الإلكترونية التي بدأت تأخذ حيزا هاما على شبكة الإنترنت، حيث أصبحت مكانا خصبا لارتكاب هذا النوع من الجرائم[5].
- **المدونات ومجموعات الأخبار *(news groups)*** : وهي عبارة عن مناطق مناقشات عامة عبر الإنترنت حول مواضيع متفرقة، مع إمكانية تبادل الصور والمعلومات المقروءة أو المكتوبة ويتم

---

[1] عادل عزام سقف الحيط، المرجع السابق، ص ص212–213.

[2] تعني كلمة *(site)* موقع: عقلا إلكترونيا ذو سعة كبيرة مرتبط بشبكة الإنترنت قصد استقبال وتخزين وتوزيع المعلومات، ويتطلب إنشاء موقع انترنيت خادم ويب ومحتوى معلوماتي، والموقع الإلكتروني: هو عبارة عن مواد معلوماتيّة يمكن أن تحتوي نصوصاً أو صوراً أو رسومات أو مواد سمعية أو بصرية ثابتة أو متحركة كالأغاني، أو مقاطع الفيديو. ويتم إنشاء وتصميم الموقع الإلكتروني بلغات برمجية خاصّة يفهمها الكمبيوتر، ويتم تحميله على شبكة الإنترنت باستخدام برامج خاصة وتطبيقات معينة، راجع، حسين بن سعيد الغافري السياسة الجنائية، المرجع السابق، ص86.

[3] زيدان زيبحة، المرجع السابق، ص83.

[4] ومن أشهر قضايا الإساءة استخدام المنظمات النازية لشبكة الإنترنت لنشر أفكارها العنصرية حيث زودت بعض مواقعها بمواد سمعية بصرية، وكتابات فاشية، كما تضمنت قوائم بأسماء وعناوين الشخصيات اليسارية الألمانية لتحريض أعضاءها على استخدام التصفية الجسدية. راجع، محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن ط1 2007، ص40.

[5] المرجع نفسه، ص38.

ذلك من خلال نظام نيوز جروب *(news groups)*أو نظام يوزنت *(Usenet)*، وكلاهما عبارة عن مجموعات أخبار. أما المدونة فهي صحيفة إلكترونية شخصية يحرّرها أصحابها بصفاتهم الفردية أو الجماعية ويعرضون فيها أفكارهم ووجهات نظرهم في الأمور العامة أو الخاصة[1]. نجد أن صور الذم والقذف والتحقير يمكن أن تمارس خلال مجموعات الأخبار، فيكون وجاهيا متى كان كل من الجاني والمجني عليه يتبادلون الرسائل عبر أو بصدد تعليقهم على موضوع معين. حيث تُنشر وتُذاع عبارات الذم والقذف والتحقير بين الجمهور عبر حلقات النقاش هذه، أو قد توزع على فئة منهم على شكل كتابات أو صور أو رسوم...إلخ[2].

- **البريـد الإلكتروني*(e-mail)*:** وهو أكثر استخدامات الإنترنت شيوعا يتكون من جزئين رئيسين هما: رأس*(header)* ونص*(body)*، حيث يحتوي الرأس على معلومات حول المرسل والمتلقي والمعلومات اللاّزمة لتوصيل الرسالة للشخص المناسب، بينما يحتوي النص على الرسالة التي تم تكوينها ثم تنقل إلى ملقم البريد*(Mail Server)* والذي يوجد به صندوق المرسل. وعندها يستطيع المرسل إليه استرجاع محتويات صندوق بريده الإلكتروني عند اتصاله بالخادم الخاص به يستطيع الجاني من خلال البريد الإلكتروني إرسال الكتابات والرسوم والصور الإستهزائية، فيتسلمها عدد غير محدود من المتعاملين مع الإنترنت، ويستوي أن يتم النشر من مكان عام أو خاص وسواء من الجاني أو بناء على طلب الغير وسواء عن طريق تداول نسخة واحد من البريد أو عدة نسخ والمهم هو الاعتداء على كرامة الشخص واعتباره من خلال فحوى الرسالة[3].

- **مواقع التواصل الاجتماعي وغرف الدردشة:** تمكن هذه المواقع مستعمل شبكة الإنترنت من إنشاء صفحة خاصة به باستعمال معلومات في الغالب تكون مزيفة، أو بإنشاء صفحة تسمى (مجموعة) *(Groupe)*، تمثل مجموعة من الأشخاص يشتركون في أفكار متقاربة، أو تجمعهم مهنة معينة، وتتم الجريمة بنشر مقالات أو صور أو رسوم كاريكاتورية أو نشر تعاليق الهدف منها النيل من شرف واعتبار الآخرين[4]. في هذا الصدد، نذكر قضية المدون الجزائري (ع.غ.ع) الذي تُوبع في سنة 2015 من أجل جريمة "إهانة وقذف هيئات نظامية عن طريق الكتابة في مواقع التواصل الاجتماعي، حيث قام بنشر رسومات تسيئ إلى رئيس الجمهورية والوزير الأول، وهذا عبر موقع التواصل الاجتماعي*(Facebook)*[5].

---

[1] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، مصر، ط1، 2009، ص100.

[2] محمد أمين الشوابكة، المرجع السابق، ص42.

[3] عادل عزام سقف الحيط، المرجع السابق، ص ص204-205.

[4] مصطفى محمد موسى، التحقيق الجنائي، المرجع السابق، ص102.

[5] لأكر تفاصيل حول هذه القضية ، يرجى الدخول على الموقع الرسمي لمحرك البح الجزائري جزايرس *(djazairess)* على الرابط الآتي: *http://www.djazairess.com/essalam/42690*، تاريخ الاطلاع: 2016/10/18 على الساعة:21:15.

- **من خلال الهاتف النقال*(Cellular)*:** لم تعد الثورة الرقمية تقتصر على التبادل الإلكتروني للبيانات بين الحواسيب سواء على مستوى الشبكة المحلية أو على مستوى الشبكة العالمية، بل أصبح من الممكن الدخول إلى شبكة الإنترنت من خلال الهاتف المزود بشريحة ذكية، حيث يستطيع الاتصال بشبكة الإنترنت وتبادل رسائل *(SMS,MMS)*، وإرسال واستقبال رسال عبر البريد الإلكتروني، وبالتالي يمكن ارتكاب جرائم الإهانة والسب والقذف في حق الأشخاص والمؤسسات على حد السواء، والأمر نفسه ينطبق على استعمال اللوحة الرقمية *(Tablette Numérique)*[(1)].

هـ -الركن المعنوي: جريمة الإهانة جريمة عمدية تتطلب القصد الجنائي العام الذي يقوم على العلم والإرادة والقصد الجنائي الخاص، فيجب توافر علم الجاني بصفة الضحية واستهدافه اعتبارا لتلك الصفة، وقصدا خاصا يتمثل في نية المساس بشرفه واعتباره وبالاحترام الواجب لسلطته.

و-العقوبات المقررة: الحبس من (3) أشهر إلى اثني عشر(12) شهرا وبغرامة من 50.000 دج إلى 250.000دج، و في حالة العود تضاعف عقوبة الحبس والغرامة.

كما تجدر الإشارة إلى أن المشرع عدّل من قيمة الغرامات المالية المقررة في مادة الجنح والمخالفات في حدها الأقصى والأدنى، وذلك بموجب المادة (60) من القانون رقم: 23/06 المعدل والمتمم لقانون العقوبات، حيث نصت هذه المادة على استحداث مادتين جديدتين هما: (464 مكرر-464 مكرر1) [(2)].

ثانيا: جريمة السب: يعرف السب لغة على أنه:" الشتم سواء بإطلاق اللفظ الصريح الدال عليه، أو باستعمال المعاريض التي تؤدي إليه"، ويعرف اصطلاحا بأنه: "خدش شرف شخص واعتباره عمدا، بإلصاق صفة عيب أو لفظ جارح إليه"[(3)].

أ- **الركن الشرعي:** نصت المادة (297) من (ق.ع.ج) على: "يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة".

ب- الركن المادي: يتكون من العناصر الآتية:

---

[1] محمد أمين الشوابكة، المرجع السابق، ص47.

[2] تنص المادة (464مكرر) من (ق.ع.ج) على:" ترفع قيمة الغرامات المقررة في مادة الجنح كما يأتي:

- يرفع الحد الأدنى للغرامات إلى 20.001دج ، إذا كان هذا الحد أقل من 20.000دج.
- يرفع الحد الأقصى للغرامات إلى 100.000دج ، إذا كان هذا الحد أقل من 100.000دج.

-يضاعف الحد الأقصى لغرامات الجنح الأخرى، إذا كان هذا الحد يساوي أو يفوق 100.000دج، ما عدا الحالات التي ينص فيها القانون على حدود أخرى".

[3] يوسف المصري، المرجع السابق، ص142.

- **خدش الشّرف والاعتبار:** يتمثل في تعبير معين يحط من قدر المجني عليه وينال من سمعته، ففعل السب يتحقق بكل ما من شأنه أن يمس بالشّرف والاعتبار دون تحقيق لواقعة محددة على خلاف القذف، فإنه لا يشترط في السب إسناد واقعة معينة للشخص وإنما يكفي أن تنطوي العبارة المستعملة على عنف وكلام ماجن أو بذيء مثل سارق أو فاسق أو لص أو مرتش ... أو مختلس أو سكّير، كما يتعين على المحكمة أن تذكر في حكمها ألفاظ السب وإلا كان حكمها مشوبا بقصور [1].
- **تعيين الشخص المقصود بالسب:** يجب أن يوجه السب إلى أشخاص معينين سواء كانوا طبيعيين أو معنويين ولا يشترط التحديد الدقيق لشخص الضحية بالاسم، بل يكفي أن يكون باستطاعة الأفراد أو بعض منهم تحديد الشخص المقصود، كما يستوي أن يوجه السب لأشخاص طبيعية أو معنوية، كما لا تقوم الجريمة إذا كانت ألفاظ السب عامة موجهة لأشخاص وهميين[2].

-**العلانية :** وهي العلانية نفسها المقررة للقذف، وتتحقق بالكتابة أو نشر الصور أو بالوسائل السمعية البصرية أو بأية وسيلة إلكترونية أو معلوماتية–كما شرحنا آنفا بخصوص تعدد الوسائل الإلكترونية والمعلوماتية في معرض حديثنا عن الركن المادي لجريمة الإهانة– أو إعلامية أخرى. فإذا كانت تقنيات الإنترنت تتيح نقل الصوت والصورة من مستخدم لآخر سواء باستعمال الوسائل الإلكترونية كالهاتف النقال أو الوسائل المعلوماتية كالحاسوب، فإنه يمكن تصور العلانية في نطاق الجرائم الإلكترونية، على أساس أنه يمكن مشاهدة الصور أو الاستماع للصوت في محل عام أو مكان مباح للجمهور أو مقاهي الإنترنت...إلخ[3]. غير أن المشرع لم يشر إلى العلانية في نص المادة (297) (ق.ع.ج) خلافا لبعض التشريعات على اعتبار أنه ليس ركنا أساسيا في جريمة السب إذ لا تنتفي الجريمة بانتفاء العلانية، وإنما تتحول من جنحة إلى مخالفة حسب نص المادة (2/463) من (ق.ع.ج) التي تنص على:" يعاقب بغرامة من 30 إلى 100 دج ويجوز أن يعاقب أيضا بالحبس لمدة ثلاثة أيام على الأكثر كل من ألقى بغير احتياط أقذارا على أحد الأشخاص.كل من ابتدر أحد الأشخاص بألفاظ سباب غير علنية دون أن يكون قد استفزه".

ج–الركن المعنوي: جريمة السب جريمة عمدية تتطلب توافر القصد الجنائي العام الذي يقوم على العلم والإرادة، وعليه يتعين ثبوت علم الجاني بالألفاظ التي صدرت عنه، وأن يكون مدركا لمعناها بأن من شأنها خدش الضحية في اعتباره، كما يجب أن تتجه إرادة الجاني إلى إتيان السلوك

---

[1] العاقد غريب أحمد، المرجع السابق، ص21.

[2] يوسف المصري، المرجع السابق، ص ص143-144.

[3] محمد أمين الشوابكة، المرجع السابق، ص51.

المادي المتمثل في تعبير مشين أو عبارة تتضمن تعبيرا أو قدحا عن طريق استعمال الوسائل الإلكترونية أو المعلوماتية وبأي وسيلة أخرى[1].

د-العقوبات المقررة: الحبس من (3) أشهر إلى اثني عشر(12) شهرا وبغرامة من 50.000 دج إلى 250.000دج، وفي حالة العود تضاعف عقوبة الحبس والغرامة.

ثالثا: جريمة القذف: القذف لغة هو: الرمي أو التوجيه، واصطلاحا هو: إسناد واقعة محددة علنيا وعمديا تستوجب عقاب من تنسب إليه، أي نسبة أمر شائن للمقذوف كازدرائه واحتقاره وبشكل علني يتوجب العقاب عليه[2].

أ-الركن الشرعي: عرفت المادة (296) من (ق.ع.ج) القذف على أنه: "يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص ، أو الهيئات المدعى عليها بها أو إسنادها إليهم، أو إلى تلك الهيئة ويعاقب على نشر هذا الادعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم ولكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة". والملاحظ أن كلا المشرعين الجزائري والمصري نصا على جريمة القذف ضمن أحكام قانون العقوبات، خلافا للمشرع الفرنسي الذي نص عليها ضمن أحكام قانون الإعلام.

ب-الركن المادي: يتكون من العناصر الآتية:

1 - **الادعاء أو الإسناد :** يختلف مدلول العبارتين، فالادعاء يحمل معنى الرواية عن الغير أو ذكر الخبر محتملا الصدق أو الكذب، بينما الإسناد يفيد نسبة الأمر إلى شخص المقذوف على سبيل التأكيد سواء كانت الوقائع منقولة عن الغير أو من تأليفه، كما لا يتحقق القذف بالإسناد المباشر فقط بل يتحقق أيضا بكل صور التعبير ولو كان ذلك بصفة غامضة[3]، ويستوي في القذف أن يسند القاذف الأمر الشائن إلى المقذوف على أنه عالم به، أو يسنده إليه بطريق الرواية عن الغير، كما لا يمنع من تحقيق الإسناد أن تكون الواقعة المسندة للضحية قد سبق نشرها أو إعلانها، ذلك أن إعادة النشر أو الإعلان تعتبر قذفا جديدا[4] .

---

[1] يوسف المصري، المرجع السابق، ص144.

[2] حسن بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص72.

[3] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، المرجع السابق، ص202.

[4] العاقد غريب أحمد، المرجع السابق، ص14.

2- **يجب أن تكون الواقعة معينة وماسة بالشرف والاعتبار:** يجب أن ينصب الادعاء أو الإسناد على واقعة ماسة بالشرف والاعتبار، وهو الفعل الذي له أثر مباشر على قيمة الإنسان سواء عند نفسه أو عند الغير، وذلك بأن يحط من كرامته أو شخصيته، ولا يكفي أن تكون هذه الواقعة شائنة وإنما يجب أن تكون معينة ومحددة، وبهذا الشرط يتميز القذف عن السب ويعد قاذفا من أسند إلى موظف تلقيه الرشوة[1] .

3 - **تعيين الشخص أو الهيئة المقذوفة :** ويستوي في ذلك أن يكون شخصا طبيعيا أو معنويا كما يجب تعيين الشخص المقذوف، ولا يشترط ذكر الاسم أو تعيينه صراحة، بل يكفي تحديد شخصيته بغير ذلك من الأمارات كالمهنة والزمان والمكان...إلخ. وهي مسألة تقديرية تناط بقاضي الموضوع[2].

4- **العلانية :** ويقصد بها اتصال علم الجمهور بالتعبير الصادر عن فكرة المتهم الذي فحواه عبارات وألفاظ شائنة تم التعبير عنها بالقول أو الفعل أو الكتابة ، أو بأية وسيلة أخرى من وسائل التعبير عن الرأي أو المعنى، ونعني هنا كافة الوسائل الإلكترونية والمعلوماتية كإرسال الرسائل النصية والصوتية وملفات الفيديو عن طريق الهاتف النقال أو بالبريد الإلكتروني. إضافة إلى نشر الصور والتعاليق والفيديوهات الساخرة على شبكة الإنترنت بواسطة المواقع الإلكترونية أو مواقع التواصل الاجتماعي...إلخ. وعموما بأي وسيلة كانت – كما سبق شرحه- وعلى هذا الأساس تعتبر العلانية الركن المميز لجنحة القذف والعلة من ذلك علم أفراد المجتمع بالعبارات المشينة الماسة بشرف واعتبار الفرد، وهي تمثل أساس العقاب عليها لأن خطورة هذه الجريمة لا تكمن في العبارات المشينة فحسب، وإنما في إعلامها للجمهور[3]، لذا يتعين على القاضي أن لا يكتفي بذكره في الحكم بأن الجريمة وقعت علنا دون أن يعين وسيلة العلانية، لكي يتسنى لمحكمة النقض المراقبة.

ج- الركن المعنوي: جريمة القذف جريمة عمدية تتطلب القصد الجنائي العام الذي يتحقق متى نشر القاذف أو أذاع الأمور المتضمنة للقذف، وهو يعلم بمعناها وأنها تمس المقذوف في شرفه أو اعتباره واحتقاره عند أهل وطنه. كما لا يشترط أن يكون القاذف حسن النية أي: معتقدا صحة ما رمى

---

[1] حسين بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص83.

[2] العاقد غريب أحمد، المرجع السابق، ص15.

[3] حسين بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص83.

المجني عليه به من وقائع القذف ولا يجوز للمتهم أن يتذرع بالاستفزاز للإفلات من العقاب، ذلك أن العبارات القاذفة لا تفقد طبيعتها حتى وإن كانت ردا على عبارات قاذفة أخرى[1].

د-العقوبات المقررة: الحبس من (3) أشهر إلى اثني عشر(12) شهرا وبغرامة من 50.000 دج إلى 250.000دج، وفي حالة العود تضاعف عقوبة الحبس والغرامة.

الفرع الثاني: جرائم الإهانة أو السب أو القذف في حق مؤسسات الدولة:

تقوم هذه الجرائم على ما يأتي:

أولا: الركن الشرعي: في هذا الشأن نصت المادة (146) من (ق.ع.ج) على:" تطبق على الإهانة أو السب أو القذف الموجهة بواسطة الوسائل التي حددتها المادة (144 مكرر) ضد البرلمان أو أحد غرفتيه أو ضد الجهات القضائية أو ضد الجيش الشعبي الوطني أو أيه هيئة نظامية أو عمومية أخرى، العقوبات المنصوص عليها في المادة المذكورة أعلاه. وفي حالة العود تضاعف الغرامة".

ثانيا: الركن المادي: تفاديا للتكرار، سنتطرق فقط إلى صفة المجنى عليهم، على اعتبار أننا تطرقنا إلى الركن المادي والمعنوي والعقوبات المقررة لكل من جريمة الإهانة والسب والقذف في الفرع الأول.

أ- **صفة المجني عليه:** حددت المادة (146) صفة المجني عليهم الذين ترتكب ضدهم الجرائم الماسة بالشرف والاعتبار وهم:

✓ **البرلمان أو أحد غرفتيه:** نصت المادة (112) من التعديل الدستوري المؤرخ في:2016/03/06 على: "يمارس السلطة التشريعية برلمان يتكون من غرفتين، وهما المجلس الشعبي الوطني ومجلس الأمة. وله السيادة في إعداد القانون والتصويت عليه".

✓ **الجهات القضائية:** نصت المادة (02) من القانون رقم:05-11 المؤرخ في:2005/07/17 المتعلق بالتنظيم القضائي على: "التنظيم القضائي يشمل النظام القضائي العادي والنظام القضائي الاداري ومحكمة التنازع"، وعليه يشمل النظام القضائي العادي المحكمة العليا والمجالس القضائية والمحاكم، كما يشمل النظام القضائي الاداري مجلس الدولة والمحاكم الإدارية[2].

✓ **الجيش الوطني الشعبي:** وهي مؤسسة الجيش الوطني الشعبي.

---

1 محمد فتحي محمد أنور عزت، تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبارات التي تقع بواسطتها-دراسة مقارنة، المركز القومي للإصدارات القانونية، القاهرة، مصر، ط1، 2012، ص241.

2 المادتان (03) و(04) وما بعدهما من القانون رقم:05-11 المؤرخ في:2005/07/17 المتعلق بالتنظيم القضائي، (ج. ر) رقم:51 المؤرخة في:2005/07/20، ص6 وما بعدها.

✓ **الهيئات النظامية أو العمومية:** تتمثل الهيآت النظامية في سلك الدرك، الشرطة...إلخ، كما تنقسم الهيئات العمومية إلى هيآت عمومية ذات طابع إداري وهيئات عمومية ذات طابع تجاري وصناعي.

لقد أصاب المشرع الجزائري في سياسته الجنائية المتعلقة بمكافحة الجرائم الإلكترونية، حينما أدرج استعمال الوسائل تقنية المعلومات وشبكات الاتصال في جرائم الشرف والاعتبار التي تقع على الأشخاص الطبيعية أو المعنوية على حد سواء، وذلك إدراكا منه بخطورة هذه التكنولوجيا وانتشارها بين أفراد المجتمع وسهولة استعمالها وسرعة انتقال المعلومات، وذلك حينما يتم إساءة استخدامها، كما تجدر الإشارة إلى أن هذه الوسائل تشكل أيضا جرائم الصحافة بموجب نص المادة (144مكرر1) من (ق.ع.ج).

لم يكتف المشرع الجزائري بتجريم الأفعال الماسة بالاعتبار والشرف فقط، وذلك عن طريق استعمال الوسائل الإلكترونية أو المعلوماتية أو الإعلامية، بل تعدى ذلك إلى تجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، نظرا لما يشكله هذا المجال من أهمية كبرى، فما هي هذه الجرائم؟ هذا ما سنتعرف عليه في المطلب الموالي.

المطلب الثاني: جرائم المساس بأنظمة المعالجة الآلية للمعطيات ومدى كفاية القانون رقم: 04-15 لتجريمها

تعد القدرة العملية على خلق ومعالجة وتخزين ونقل المعلومات الرقمية من أكبر ما انتجته تكنولوجيا تقنية المعلومات، فأصبحت الحواسيب والشبكات التي تربط فيما بينها بصورة سريعة جدا قوة سائدة في مجالات عديدة، كقطاع الأعمال الحكومي والخاص والتعليم والترفيه...إلخ. لذا يعتبر قطاع خدمات ومنتجات المعلومات من أكبر القطاعات الاقتصادية في العالم، إذا يحقق عائدات تبلغ 3.5 تريليون دولار أمريكي[(1)].

في ظل هذه الطفرة التكنولوجية برزت أشكال جديدة من الجرائم المستحدثة، مما دفع بالكثير من الدول إلى النص على معاقبتها، وأن الجزائر على غرار هذه الدول تسعى إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات. على إثر هذا قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم:04-15 المؤرخ في:10 نوفمبر2004، بإضافة قسم سابع مكرر تحت عنوان" جرائم المساس بأنظمة المعالجة الآلية للمعطيات" من المواد(394 مكرر إلى 394مكرر7)، تماشيا في ذلك مع الاتجاه العالمي لمكافحة هذا النوع المستحدث من الجرائم بكافة

---

[1] فريد هـ.كيت، الخصوصية في عصر المعلومات، ترجمة، محمد محمود شهاب، مركز الأهرام للترجمة والنشر، القاهرة، مصر، ط1 1999، ص17.

أشكاله. سنتطرق إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات والعقوبات المقررة لها بما فيها عقوبة الشخص المعنوي في (الفرع الأول).ثم نتناول مختلف أشكال الاعتداءات الأخرى على أنظمة المعالجة الآلية للمعطيات ومدى كفاية القانون رقم: 04-15 لتجريمها في (الفرع الثاني).

الفرع الأول: جرائم المساس بأنظمة المعالجة الآلية للمعطيات:

إن دراسة هذه الجرائم تقتضي منا أولا توضيح مفهوم "نظام المعالجة الآلية للمعطيات"، على اعتبار أنه شرط مفترض لقيام هذه الجرائم، إضافة إلى طرح التساؤل الآتي: هل يشترط في هذه الجرائم خضوع نظام المعالجة الآلية للمعطيات للحماية الفنية؟.

أولا: تعريف نظام المعالجة الآلية للمعطيات: إن نظام المعالجة الآلية للمعطيات تعبير فني يصعب على الباحث في مجال القانون إدراك حقيقته وفحواه بسهولة. فضلا على كونه مفهوما متطورا يخضع للتطورات السريعة في مجال صناعة تكنولوجيات الإعلام والاتصال[1]، عرفته المادة (01/أ) من (إ.أ.م.إ.م) على أنه:" أيُّ جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة، يقوم واحدا منها أو أكثر بالمعالجة الآلية للمعطيات تنفيذا لبرنامج معين"[2]. كما يعرف أيضا على أنه:" كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون منها الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي يربط بينها مجموعة من العلامات التي يتم عن طريقها تحقيق نتيجة معينة، وهي معالجة المعلومات على أن يكون هذا المركب خاضع لنظام المعالجة الفنية"[3].

تجدر الإشارة إلى أن المشرع الجزائري عند تناوله للجرائم الإلكترونية، سواء في قانون العقوبات أو في قانون الإجراءات الجزائية أو في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، استخدم مصطلحين اثنين مترادفين بخصوص النظام المعلوماتي هما مصطلح" نظام المعالجة الآلية للمعطيات" ومصطلح" منظومة معلوماتية". حيث عرفت المادة (02/ب) من القانون رقم: 09-04 المؤرخ في:2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم

---

[1] علي عبد القادر القهوجي، المرجع السابق، ص110.

[2] ***Article 1 – Définitions***

Aux fins de la présente Convention, l'expression:

a. «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données…, convention européenne de la cybercriminalité, Op.Cit,p.3.

[3] عبد الفتاح بيومي حجازي، الجرائم المستحدثة، المرجع السابق، ص477، راجع أيضا، محمد خليفة، جريمة التواجد، الأطروحة السابقة ص ص81-83.

المتصلة بتكنولوجيات الإعلام الاتصال، المنظومة المعلوماتية على أنها:" نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، الملاحظ أن هذا التعريف يتفق مع نص المادة (01/ب) من (إ.أ.م.إ.م)، بما يبين مدى تأثر المشرع الجزائري بنصوص هذه الاتفاقية في وضع النصوص القانونية التي تحكم الجرائم الإلكترونية سواء على مستوى التجريم والعقاب أو على المستوى الإجرائي، كما يتفق أيضا مع نص المادة (5/02) من (إ.ع.م.ج.ت.م)، حيث عرفت النظام المعلوماتي على أنه:" "مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات".

بالمقابل لم يعرف المشرع الفرنسي نظام المعالجة الآلية للمعطيات وترك ذلك للفقه الذي عرفه على أنه:" كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات، التي عن طريقها تتحقق نتيجة معينة ". ومنه يتكون نظام المعالجة الآلية للمعطيات من العناصر الآتية[1]:

- **العنصر الأول:** يتمثل في مجموعة مكونات النظام، أي المكونات المادية والمعنوية (كوحدات المعالجة، أو وحدات التخزين، أو وحدات الإدخال والإخراج...إلخ).

- **العنصر الثاني:** وجود شبكة من الاتصالات بين هذه الوحدات والعناصر: ويعني ذلك ضرورة ارتباط تلك الوحدات فيما بينها، تشكل هذه الوحدات نظاما معلوماتيا واحدا، أو مرتبطا بمجموعة من النظم الأخرى متصلة فيما بينما بواسطة أجهزة الربط المختلفة، والتي تهدف في الأخير إلى تحقيق عمل معين[2].

- **العنصر الثالث:** وجود حماية فنية: ويعني ذلك ضرورة خضوع هذا النظام للحماية الفنية حتى يتمتع بالحماية القانونية الجنائية[3]، إذ يتطلب الكم الهائل من تبادل المعلومات والرسائل خاصة عبر شبكة الإنترنت تأمينها من مختلف الجرائم الإلكترونية الواقعة عليها كالاختراق والسرقة والمحو والتعديل...إلخ، و ذلك باستعمال أسلوب التشفير مثلا.

ثانيا: مدى خضوع نظام المعالجة الآلية للمعطيات للحماية الفنية: تنقسم الأنظمة المعلوماتية إلى أنظمة مفتوحة للجمهور، وأنظمة قاصرة على أصحاب الحق فيها دون حماية فنية لها، وأنظمة قاصرة على أصحاب الحق فيها، لكنها تتمتع بحماية فنية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها، وذلك من خلال توفير الأدوات والوسائل اللازم لحماية المعلومات من المخاطر

---

1 محمد حماد مرهج الهيتي، الجريمة المعلوماتية، المرجع السابق، ص164، راجع أيضا، *Myriam Quéméner et Yves Charpenel,Op.Cit,p.59,et aussi , Nidal El Chaer,Op.Cit,p.97.*

2 محمد حماد مرهج الهيتي، الجريمة المعلوماتية، المرجع السابق، ص199.

3 علي عبد القادر القهوجي، المرجع السابق، ص112.

الداخلية أو الخارجية [1].أما من الجانب الفقهي، فلقد برز اتجاهان متعارضان حول مسألة اضفاء الحماية الفنية على النظام المعلوماتي من عدمها:

– **الاتجاه المؤيد للحماية الفنية:** يرى أصحاب هذا الاتجاه أنه من الطبيعي حماية النظام المعلوماتي بسبب أنه من يقوم بالاستغلال وجب عليه وضع الوسائل الفنية اللازمة للحماية من الغش المعلوماتي، وأن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم[2].

– **الاتجاه المعارض للحماية الفنية:** بينما لا يشترط أصحاب الاتجاه المعارض وجود الحماية الفنية بسبب أن المشرع لم ينص على ذلك، وأنه لا يجوز أن تقتصر الحماية الجنائية على الأنظمة المحمية فقط، وإنما يجب أن تمتد لتغطى كل أنظمة المعالجة الآلية للمعطيات، كون هذا الشرط يؤدي مباشرة إلى الحد من الحماية الجنائية للنظم غير المشمولة بتجهيزات أمنية داخل النظام[3]. غير أن تعريف مجلس الشيوخ الفرنسي للنظام المعلوماتي، والذي يوافق الفقه الراجح في هذا الموضوع، إضافة إلى كثير من التشريعات المقارنة لا يشترطون إضفاء حماية فنية على النظام المعلوماتي[4].

بالنسبة للمشرع الجزائري، نلاحظ من جهة أنه استعمل مصطلح" منظومة " بدلا من مصطلح "نظام" في التعريفات السابقة، وأصاب في ذلك بسبب تعدد أنواع الأنظمة المعلوماتية لا ينحصر فقط في نظام الحاسوب، بل كل نظام أو جهاز يقوم بالمعالجة الآلية للمعطيات ومنها شبكة الإنترنت والبريد الإلكتروني والبطاقة الإلكترونية كبطاقة الائتمان البنكية، وموزع النقود...إلخ. وبالتالي ترك المشرع الباب مفتوحا في سياسته الجنائية أمام ظهور منظومات معلوماتية جديدة مع تعدد استعمالاتها. ومن جهة أخرى، لم يشترط لقيام الجريمة خضوع النظام المعلوماتي للحماية الفنية شأنه في ذلك شأن المشرع الفرنسي، وبالتالي أخذ بالاتجاه الرافض لإضفاء الحماية الفنية على النظام المعلوماتي، حيث يهدف المشرع من وراء ذلك إلى اضفاء الحماية الجزائية على كافة أنظمة المعالجة الآلية للمعطيات بغض النظر عن تمتعها بالحماية الفنية أم لا.

ثالثا: صور الاعتداء على أنظمة المعالجة الآلية للمعطيات: تعد أنشطة الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات من أكثر الجرائم شيوعا آخرها قضية اختراق موقع جامعة باجي مختار بعنابة برسم الدخول الجامعي لسنة2016/2015 من أجل التلاعب بالتسجيلات الجامعية وتوجيه العشرات من الطلبة والطالبات إلى تخصصات جامعية دون توافر الشروط

---

[1] *Alain Bensoussan, Internet, Op.Cit,p.198.*

[2] أحمد حسام طه تمام، المرجع السابق، ص265–266 ، راجع أيضا، محمد خليفة، جريمة التواجد، الأطروحة السابقة، ص139.

[3] محمد حماد مرهج الهيتي، الجريمة المعلوماتية، المرجع السابق، ص ص283–285.

[4] *André Lucas et Autre, Op.Cit,p.680, voir aussi, Nidal El Chaer,Op.Cit,p.124.*

المطلوبة[1]. حيث دفعت هذه الاعتداءات المتكررة بخصوص قرصنة مؤسسات الدولة ومنها مؤسسات التعليم العالي، السيد الوزير الأول إلى مراسلة السادة رؤساء المؤسسات الجامعية والسادة إطارات الإدارة المركزية لأخذ الاحتياطات اللازمة بخصوص قيام بعض القراصنة باستعمال طريقة التزييف *(pharming)*، والتي تتمثل في إنشاء صفحات أو عناوين مشابهة لمواقع واب المؤسسات المستهدفة حيث يجعل من الصعب التفريق بينها فيقع المستخدم ضحية هذه المواقع المزيفة[2]. من جهة أخرى تختلف الوسائل المستعملة في ذلك، من بين أكثر الوسائل استعمالا برامج الفيروسات[3]، وهو برنامج معلوماتي صغير يمتاز بخاصية الخفاء*(furtifs)*[4]. حيث يقوم المجرم المتخصص في البرمجة بوضع فيروس في النظام المعلوماتي يصعب في كثير من الأحيان اكتشافه من طرف برامج الحماية يقوم هذا الفيروس بمهام حسب الغرض المحدد له كمحو أو تعديل أو استنساخ المعطيات أو ربما أخطر من ذلك، وهو إفساد سير النظام المعلوماتي. غير أن الأمر يتطلب من المجرم الإلكتروني قدرا من المعرفة والمهارة في مجال استعمال المعلوماتية. والملاحظ أن المشرع الجزائري انسجم في تجريمه للأفعال الماسة بأنظمة المعالجة الآلية للمعطيات مع نصوص الاتفاقيات الدولية والعربية المبرمة في هذا الشأن مثل (إ.أ.م.إ.م)، و(إ.ع.م.ج.ت.م) –المشار إليها سابقا– نظرا لطبيعة هذه الجرائم المستحدثة، كما أن هناك اتجاه دولي يقضي بضرورة مكافحتها جماعيا على اعتبار انه لا تستطيع دولة بمفردها فعل ذلك.

1– جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات: تجدر الإشارة إلى أنه تستعمل عدة مصطلحات للدلالة على هذه الجريمة مثل: الدخول عن طريق الغش، والدخول غير المصرح به، القرصنة أو الاختراق، الدخول والبقاء الاحتيالي في الأنظمة المعلوماتية، الدخول

---

[1] القضية لازالت مطروحة أمام محكمة عنابة، ولم يصدر فيها حكم بعد.

[2] مراسلة السيد الوزير الأول رقم:2981 المؤرخة في:2016/09/22، المتعلقة بقرصنة معلومات تستهدف مؤسسات الدولة، منشورة على الموقع الرسمي لجامعة باجي مختار عنابة على الرابط الآتي:*http://www.univ-annaba.dz/component/k2/item/485-bulletin-d-information-relatif-%C3%A0-une-forme-de-piratage-informatique-ciblant-les-institutions-de-l-%C3%A9tat.html*، تاريخ الاطلاع:2016/10/07 على الساعة:09:37.

[3] قضية (دودة مورس): وقعت الحادثة سنة 1988، تعتبر من الهجمات الكبيرة والخطرة في بيئة الشبكات، حيث تمكن طالب يبلغ من العمل 23 عاما ويدعى: *(ROBER MORRIS)* من اطلاق فيروس عرف باسم (دودة مورس) عبر الإنترنت، أدى إلى إصابة 6 آلاف جهاز يرتبط معها حوالي 60000 نظام عبر الإنترنت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار، إضافة إلى مبالغ أكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة، وقد حُكم عليه بالسجن لمدة 3 أعوام وعشرة آلاف دولار غرامة، راجع، يوسف حسن يوسف المرجع السابق، ص ص 50–51.

[4] هدى حامد قشقوش، المرجع السابق، ص99، راجع أيضا، هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص158، محمد علي العريان، المرجع السابق ، ص 103، عبد الحكيم رشيد توبة، المرجع السابق، ص171.

دون حق. كما يمكن تعريف هذه الجريمة على أنها:" الولوج داخل النظام المعلوماتي أو البقاء فيه بغير تصريح من المسؤول عنه، وذلك إضرارا إما بسرية أو سلامة أو تكامل أو موفورية هذا النظام ومحتوياته"[1].

أ-**الركن الشرعي:** تنص المادة (394 مكرر) (ق.ع.ج) على: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6)أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150000 دج".

نلاحظ أن هناك تقريبا تطابقا كليا بين هذه المادة ونص المادة(1/323) من (ق.ع.ف)[2] يظهر لنا ذلك مدى تأثر المشرع الجزائري بنظيره الفرنسي في مجال التشريع. كما نصت عليه المادة (02) من (إ.أ.م.إ.م)[3]، وأيضا المادة (06) من (إ.ع.م.ج.ت.م)[4].

بالنسبة لجرائم الاعتداء على نظم المعالجة الآلية للمعطيات، لابد أن نكون بصدد نظام المعالجة الآلية للمعطيات، وهو بمثابة الشرط المفترض لقيام هذه الجرائم، وعلى سبيل المثال، فإذا كنا

---

[1] محمد خليفة، جريمة التواجد، الأطروحة السابقة، ص15.

[2] ***Article 323-1 du (CPF) :***

"Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende".

[3] ***Article 2 - Accès illégal***

"Chaque Partie adopte les mesures législatives…, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques…", convention européenne de la cybercriminalité, Op.Cit,p.3.

[4] تنص المادة (06) من (إ.ع.م.ج.ت.م) على:" الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين - الحصول على معلومات حكومية سرية".

بصدد الاعتداء على معطيات تتعلق بالتجارة الإلكترونية فلا بد أن نكون بصدد منظومة معلوماتية تتعلق بالنظام المذكور وبأطرافه وهي تفرض الارتباط بوسيلة اتصالات حديثة[1] .

ب–الركن المادي: يكون الفعل الجرمي في صورتين: صورة بسيطة تتمثل في مجرد الدخول أو البقاء غير المشروع، وصورة مشددة حينما تقترن بحذف أو تغيير المعطيات الموجودة في المنظومة أو تخريب لنظام اشتغال المنظومة. كما تجدر الإشارة إلى أن المشرع الجزائري لم يعرف فعل الدخول أو البقاء في هذه الجريمة.

ب1–الصورة البسيطة:

• **فعل الدخول*(L'accès)*:** لا يقصد بالدخول المعنى المادي، وإنما الدخول وبطريق الغش إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات، وسواء كان الدخول جزئيا أو كليا، وذلك باستعمال الوسائل الفنية أو التقنية اللازمة[2]. كما تتسع هذه العبارة على إطلاقها لتشمل كافة فنيات الدخول الاحتيالي في منظومة محمية كانت أو غير محمية[3]، فيمكن تعريف الدخول على أنه: "عملية غير مصرح بها إلى أجهزة الغير وشبكاتهم الإلكترونية"[4]، أو هو: "الدخول لمنظومة معلوماتية كليا أو جزئيا وسواء كانت عامة أو خاصة بهدف الاحتيال المعلوماتي...إلخ[5] أو هو: "إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له استخدامه، للوصول إلى المعطيات والمعلومات المخزنة بداخله للطلاع عليها او لمجرد التسلية ، أو لإشباع الشعور بالنجاح في اختراق الحاسب الآلي[6].

ويتم الاختراق[7] بكافة أنواعه، بواسطة برامج متطورة يستخدمها القراصنة أو كل من يملك خبرة في استعمالها مثل: القنابل المنطقية أو الفيروسات كحصان طروادة أو بواسطة الإغراق

---

[1] عبد الفتاح بيومي حجازي، الجرائم المستحدثة، المرجع السابق، ص477.

[2] زينات شحادة، المرجع السابق، ص46 .

[3] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، المرجع السابق، ص453.

[4] خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص242.

[5] *Nidal El Chaer,Op.Cit,pp.111-112.*

[6] محمد خليفة، جريمة التواجد، الأطروحة السابقة، ص142.

[7] ينقسم الاختراق إلى ثلاثة أنواع:

– اختراق الأجهزة الخادمة: ويتم عن طريق المحاكاة باستخدام مسارات المصدر، وفيها يتم اعطاء حزم عناوين*(IP)* شكلا معينا لتبدو وكأنها صادرة من حاسوب مصرح له بالدخول.

– التعرض للبيانات أثناء انتقالها: وتتم هذه الطريقة بالتعرف على أرقام بطاقات الائتمان أثناء استعمالها من طرف العميل في مراكز التسوق، والبنوك...إلخ.

– اختراق الأجهزة الشخصية: وهي الطريقة الأكثر شيوعا نظرا لتوفر السوق على العديد من برامج الاختراق. المرجع نفسه، ص114.

بالرسال[1]، أو عن طريق ما يعرف بالصيد *(fishing)* باستعمال برامج احتيالية *(programme de spamming)*، حيث يقوم الجاني باستعمال هوية شركة وبريدها الإلكتروني بإرسال رسالة إلكترونية للمجني عليه يطلب منه حجز بياناته البنكية، ثم يقوم الجاني باستعمال هذه البيانات لسحب أموال المجني عليه[2]. وعليه يتم الدخول إلى النظام بأي وسيلة تقنية كانت، سواء كان ذلك عن طريق استعمال كلمة السر الحقيقية متى كان الجاني غير مخول في استخدامها أو عن طريق استعمال برامج وشفرة خاصة [3]. كما أن للقرصنة مخاطر كبيرة أهمها الحصول على المعلومات من الكمبيوتر بصورة غير مشروعة مثل: نسخ البرامج، اختراق قواعد البيانات، اختراق البريد الإلكتروني، اختراق حسابات مواقع التواصل الاجتماعي*(facebook,twitter)*...إلخ[4]، حيث بات يشكّل هذا الأمر تهديدات جدّية على حرمة الحياة الخاصة للأفراد.

من جانب آخر، لم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام ولذلك تقع الجريمة بأية وسيلة أو طريقة، فقد يكون عن طريق برنامج فيروس أو عن طريق استعمال الرقم الكودي *(Code)* لشخص آخر، أو عن طريق تجاوز نظام الحماية خاصة إذا كان ضعيفا[5]. ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر[6]. كما أن هذه الجريمة ليست من الجرائم

---

[1] الاغراق بالرسائل: هي إحدى طرق اختراق الحاسوب، تتم بإرسال كم هائل من الرسائل عبر البريد الإلكتروني بهدف تعطيل الحاسوب عن العمل، تتسبب هذه الرسائل في غلق منافذ الاتصال وملئ قوائم الانتظار، لتفاصيل أكثر في الموضوع، راجع، منير محمد الجنبيهي وممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر، 2004، ص58 راجع أيضا، يوسف حسن يوسف، المرجع السابق، ص101 وما بعدها.

[2] *David FOREST et Gautier Kaufman, Op.cit,p.95, voir aussi, Myriam Quéméner et Joel Ferry, Op.Cit,p.83, et aussi, Ali EL AZZOUZI, Op.Cit,pp.48-50.*

[3] عبد الفتاح بيومي حجازي، الجرائم المستحدثة، المرجع السابق، ص483.

[4] نعيم مغبغب، مخاطر المعلوماتية والإنترنت-المخاطر على الحياة الخاصة وحمايتها-دراسة مقارنة، (ب.د.ن)، 1998، ص221 وما بعدها.

[5] علي عبد القادر القهوجي، المرجع السابق، ص120.

[6] ومن أكثر التقنيات استعمالا لتحقيق الدخول إلى النظام :

- استخدام البرامج المصممة أصلا لاختراق أنظمة الحماية *(Protection Systems)*.
- الفخ (*la trappe*) : وهو عبارة عن منفذ يجهز به النظام مسبقا من قبل مصمم النظام ليسمح له لاحقا بإنزال برامج تعيق سير عمله.
- التخفي *(déguisement)* : ويعني انتحال صفه من له الحق في الدخول إلى النظام ثم الحصول على امتيازاته في الاطلاع على المعلومات.
- القناة المخفية *(canal cache)* : وهو من أخطر الاعتداءات ويتطلب ذكاء فائقا من المعتدي لاختراق سياسة الأمن والحماية المعتمدة في الأنظمة المعلوماتية لتهريب المعلومات.
- التسلّل *(faufulement):* ومعناه التسلل وراء مستعمل مرخص له بالدخول إلى نظام معلوماتي وتخطي حاجز الدخول.
- كسر كلمات المرور عن طريق الاستيلاء عليها من أصحابها الشرعيين==.

التي تتطلب صفة معينة، فبإمكان أي شخص القيام بها سواء كانت له علاقة بالنظام المعلوماتي أم لا.

من جهة أخرى لكي تقوم الجريمة لا بد أن يكون الدخول دون تصريح، مما يطرح سؤالا حول من يصرح بالدخول؟ إذ تتوقف الجريمة على إرادة الشخص أو الهيئة الذين يملكان السيطرة على النظام. في هذا الشأن عرفت المادة (02) من الاتفاقية لخاصة بحماية الأفراد في مواجهة نظم المعالجة الآلية للمعطيات ذات الطابع الشخصي، والتي تبناها المجلس الأوروبي بتاريخ: 28 جانفي1989 الشخص المصرح بالدخول:" كل شخص طبيعي أو معنوي، أو كل سلطة عامة أو كل مؤسسة أو جهاز يكون لهم سلطة التصرف في نظام الحاسب الآلي التابع لهم وتقرير مضمونه أو محتواه، وكيفية تنظيمه والهدف منه"[1]. ويلاحظ أن غالبية جرائم الدخول أو البقاء غير المشروع تتم من خلال برامج متوفرة على شبكة الإنترنت، تمكّن كل شخص له خبرة بسيطة في المعلوماتية شن هجمات على هذه الأنظمة وهنا تكمن الخطورة، كما يعاقب عليهما بغض النظر عن حسن نية الجاني والنتيجة المحققة[2].

- **فعل البقاء *(Maintient)***: ويقصد به: "حالات التواجد غير المصرح به في النظام المعلوماتي كربط الاتصال والاطلاع على البيانات أو القيام بعملية مختلفة"[3] أو هو: "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام"[4]، كما يتسع فعل البقاء ليشمل أكثر من الوقت المحدد وذلك بقصد عدم أداء إتاوة، وعليه يجرم فعل البقاء حتى ولو حصل بصفة عرضية[5]. قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول على النظام كما قد يجتمعان. ويكون البقاء معاقبا عليه استقلالا حينما يكون الدخول إلى النظام مشروعا مثل الدخول إلى النظام صدفة أو عن طريق لخطأ أو السهو، فهذه الصورة تحقق السلوك المجرم

==- حصان طروادة *(cheval de Troie)*: وذلك بواسطة إرسال ملف باتش *(patch)* صغير بالبريد الإلكتروني، وما إن يقوم المرسل بفتحه يتم اختراق النظام، أو عن طريق أبواب المصيدة، أو عن طريق صناديق القمامة، أو عن طريق المنافذ المفتوحة أو بواسطة أنظمة فك الشيفرات...إلخ، رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 1، 2009، ص17. راجع أيضا، حسين بن سعيد الغافري، السياسة الجنائية المرجع السابق ، ص334 و ما بعدها، وأيضا،*Myriam Quéméner et Joel Ferry, Op.Cit,p.75*

[1] محمد خليفة، جريمة التواجد، الأطروحة السابقة، ص148.

[2] خالد ممدوح إبراهيم، أمن الجريمة، المرجع السابق، ص85 ، راجع أيضا، *Alain Bensoussan ,Internet, Op.Cit,p.199*

[3] *Alain Bensoussan, L'informatique, Op.Cit,p.372.*

[4] زينات شحادة، المرجع السابق، ص48 ، راجع أيضا، محمد خليفة، جريمة التواجد، الأطروحة السابقة، ص158.

[5] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، المرجع السابق، ص453.

لفعل البقاء، وهي من جرائم النشاط الإيجابي الذي يتحقق بالامتناع أو الترك فيجب على الجاني في هذه الحالة قطع الاتصال الذي تحقق عن طريق لخطأ والانسحاب فورا[1].

ويكون البقاء جريمة أيضا إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية والاطلاع فقط . وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا، حينما لا يكون للجاني الحق في الدخول إلى النظام ، ويدخل إليه فعلا ضد إرادة صاحبه[2].

يتضح لنا أن هدف المشرع هو حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة وغير مباشرة، وأيضا حماية المعطيات والبيانات الموجودة داخله[3]، وحسنا فعل نظرا للقيمة المستحدثة للمعلومات في شتى المجالات.

ب2-الصورة المشدّدة: تنص المادة (394 مكرر/3/2) (ق.ع.ج)على:"... تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6)أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150000 دج".

وعليه تتحقق هذه الصورة عندما ينتج عن فعل الدخول أو البقاء إما حذف (محو) أو تغيير (تعديل) المعطيات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه، ففعل الحذف يشير إلى إزالة المعطيات داخل النظام، وهو أقصى أنواع الضرر مما جعل العقاب عليه مشددا، أما فعل التغيير هو إحداث تعديلات فحسب في المعطيات دون أن يصل الأمر إلى حد إزالتها، بحيث تظل المعلومة موجودة ولكن بدون معنى أو فائدة أو لها معنى ولكنه مغاير لما كانت عليه قبل التغيير. أما تخريب النظام فيقصد به كل فعل من شأنه جعل النظام مصابا بالشلل أو بالعجز، وذلك باستعمال تقنيات كثيرة منها: برامج الفيروسات كبرنامج حصان طروادة والقنبلة الموقوتة وبرامج الدودة، أو باستعمال تقنية "التشبع" *(saturation)*، أو استعمال تقنية الفخ *(trappe)...إلخ*[4]. ولتتوفر هذه الظروف المشددة، لا بد من وجود علاقة سببية بين الدخول أو البقاء غير المشروع وتلك النتيجة الضارة، إلا إذا أثبت الجاني انتفاء تلك العلاقة أو أن حذف أو تغيير المعطيات أو أن عدم صلاحية

---

[1] محمد مزاولي، المسؤولية الجنائية للأشخاص المعنوية عن الجرائم الإلكترونية في القانون الجزائري، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 1، 2009، ص30، راجع أيضا، محمد خليفة، جريمة التواجد، الأطروحة السابقة، ص159.

[2] *Nidal El Chaer,Op.Cit,pp.115-116.*

[3] زينات شحادة، المرجع السابق، ص ص48-49.

[4] رشيدة بوكر، المرجع السابق، ص231، راجع أيضا، زينات شحادة، المرجع السابق، ص62.

النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ، فحينئذ يعاقب على أساس الصورة البسيطة لفعل الدخول أو البقاء[1].

ج-الركن المعنوي: جريمة الدخول أو البقاء داخل النظام جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة، والقصد الجنائي يثبت إلى المتهم كلما توفر عنصر الغش طالما أنه تعمد إتيان هذا الفعل وبدون ترخيص من صاحب النظام المعلوماتي[2].

وعليه يتوفر الركن المعنوي في حال علم الجاني بكافة العناصر المشكلة للجريمة، بمعنى أن فعله ينصب على نظام المعالجة الآلية للمعطيات، وأنه لا يملك حق الدخول إليه أو البقاء فيه، وأنه ينتهك سرية وخصوصية هذا النظام[3]. حيث يتبين لنا من استقراء نص المادة(394 مكرر) أن المشرع لا يتطلب وجود قصد جنائي خاص لدى الجاني حتى تقوم الجريمة، وأنه يكفي لقيامها توافر القصد الجنائي العام القائم على العلم والإرادة. من جانب آخر يمكن للقاضي الجزائي أن يستنتج بأن الجاني قام عمدا بارتكاب هذه الجريمة من خلال قرائن عديدة مثل: استعمال برامج الاختراق، وضبط المعطيات المتعلقة بالنظام المخترق بحوزة الفاعل...إلخ[4].

غير أنه لا يتوافر الركن المعنوي في حق الجاني، إذا تمّت هذه الأفعال في صورة الخطأ، لكن يجب أن يثبت الجاني أنه لم يرد الوصول لهذه النتيجة[5]، مثل اعتقاد الجاني أن دخوله أو بقاؤه داخل النظام مسموح به، كما لا يتوافر أيضا الركن المعنوي إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، أو تم ذلك عن طريق الصدفة لا سيما إذا لم تحدد صلاحيات المستعمل بدقة. لكن في المقابل لابد عليه أن يخرج فورا من النظام حال علمه بأن دخوله أو بقاءه غير مصرح به، فإذا لم يفعل ذلك توافر لديه القصد الجنائي منذ اللحظة التي تحقّق فيها العلم[6]. من جهة أخرى تتميز نظم المعالجة الآلية للمعطيات بأنها مناطق مفتوحة بعضها على

---

1 آمال قارة، المرجع السابق، 114.

2 زيدان زيبحة، المرجع السابق، ص61، راجع أيضا، محمد خليفة، جريمة التواجد، الأطروحة السابقة، ص168.

3 *Myriam Quéméner et Yves Charpenel,Op.Cit,p.72.*

4 استندت محكمة باتنة في حكمها الصادر بتاريخ:2010/06/01 على أنه:" ثبت للمحكمة من خلال أوراق القضية لاسيما الخبرة الفنية لخاصة بتحليل البريد الإلكتروني للمتهم، أنه كان يقوم بالدخول عن طريق القرصنة (الغش) باستعمال برامج متنوعة...وجمع المعطيات المعلوماتية الخاصة واستعمالها في تهديد الشركة الأمريكية في مقابل حصوله على مبال مالية..."، فعملية الدخول للمنظومة المعلوماتية كانت عن طريق الغش، وهو ما يؤكد سوء نية الجاني للحصول على هذه المعطيات لاستعمالها ونشرها مقابل مبالغ مالية، أنظر: الحكم رقم:10/05272 الصادر عن محكمة باتنة بتاريخ:2010/06/01.

5 *CHRISTIANE FERAL-SCHUHL, Le Droit à L'épreuve, Quatrième édition, Op.Cit,p.598.*

6 محمد خليفة، جريمة التواجد، الأطروحة السابقة، ص ص171-172.

بعض وبتشعب نوافذها، لذا يجب التأكد من توافر القصد الجنائي لدى الفاعل في تجاوز التصريح الممنوح له[1]. كما اعتبر المشرع الفرنسي توافر الركن المعنوي في حق شخص غير مسموح له الدخول للنظام حتى ولو قام بتلك الأفعال بحسن نية[2].

يلاحظ أن المشرع الجزائري لم يكتف بتجريم فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات، بل تجاوز ذلك إلى تجريم مجرد المحاولة حسب نص المادة(394 مكرر) (ق.ع.ج)"...أو يحاول ذلك..."، وهو تأكيد منه على خطورة هذا الفعل.

د- العقوبات المقررة:

- الصورة البسيطة: المادة (394مكرر): من 3 ثلاثة أشهر (3)إلى سنة (1)حبس و50000 دج إلى 100000 دج غرامة .
- الصورة المشددة:

-المادة (394مكرر/2): تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة.

-المادة (394مكرر/3): وتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج، إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة.

2- جريمة التلاعب في معطيات نظام المعالجة الآلية للمعطيات:

أ-الركن الشرعي: تجدر الإشارة إلى أن هذه الجريمة نصت عليها المادة (04) من (إ.أ.م.إ.م)[3] والمادة (08) من (إ.ع.م.ج.ت.م)[4]. نصت المادة(394 مكرر1) من (ق.ع.ج) على: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات و بغرامة من 500.000 دج إلى

---

[1] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة للنشر، الإسكندرية، مصر 2007، ص150، راجع أيضا، علي عبد القادر القهوجي، المرجع السابق، ص ص 136-137.

[2] *jean Larguier et Philippe Conte et Anne-Marie Larguier , Droit pénal spécial, Mémento Dalloz ,France, 13 édition ,2005, p.240.*

[3] ***Article 4 - Atteinte à l'intégrité des données***

" Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques", convention européenne de la cybercriminalité, Op.Cit,p.4.

[4] تنص المادة (08) من (إ.ع.م.ج.ت.م) المتعلقة بالاعتداء على سلامة البيانات على:" تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق..."، راجع أيضا المواد:(3 و 4 و8) من (إ.أ.م.إ.م).

2.000.000 دج، كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريقة الغش المعطيات التي يتضمنها".

ب- الركن المادي: يتمثل في أفعال: الإدخال، المحو، والتعديل.

ب1-الإدخال *(Input)*: يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أوكان يوجد عليها معطيات من قبل، ويتحقق هذا الفعل في الغرض الذي يستخدم فيه مثل: قيام الحامل الشرعي لبطاقة السحب الممغنطة باستخدام رقمه السري للدخول وسحب مبلغا من النقود أكثر من الرصيد الموجود في حسابه، أو استعمال البطاقة بعد انتهاء مدة صلاحيتها، أو بعد إلغاء البنك لها[(1)]، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب كالفيروسات والقنابل المنطقية والزمنية والتي تضيف معطيات جديدة[(2)].يعد إدخال بيانات غير معتمدة في النظام المعلوماتي من أكثر الأساليب شيوعا، وهي تمثل نصف إجمالي حالات الاحتيال المعلوماتي[(3)].

ب2-المحو *(Delete)*: يقصد به إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[(4)].

ب3-التعديل *(Modulation)*: يقصد به تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى، فقد يتم باستبدال المعلومات عن طريق التلاعب في البرامج بإمداده بمعلومات مغايرة عن تلك التي صمّم البرنامج لأجلها بواسطة برامج خبيثة[(5)].

يتضح لنا من نص المادة أن المشرع الجزائري توسع في تجريم الأفعال الواقعة على نظام المعالجة الآلية للمعطيات، ومنها ما تعلق بالتلاعب في معطيات النظام سواء بالإدخال أو المحو أو التعديل، وهذا قصد مكافحة هذا النوع من الجرائم في ظل انتشار تقنية المعلومات وتوسع مجالات استعمالها، وهذا ما يدل عليه العدد المتزايد من الجرائم الإلكترونية التي تقع في الجزائر. كما اعتبر

---

[1] عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، مصر، 2015 ص328.

[2] عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة-دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص 96.

[3] هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص58.

[4] عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، المرجع السابق، ص97، راجع أيضا، علي عبد القادر القهوجي، المرجع السابق، ص132.

[5] رشيدة بوكر، المرجع السابق، ص256، راجع أيضا، علي عبد القادر القهوجي، المرجع السابق، ص132.

المشرع الجزائري هذه الجرائم من جرائم الخطر بغض النظر عن تحقيق نتيجة مادية محسوسة، لأن الجاني يقوم بالعدوان المحتمل والتهديد بالخطر في سرية المعلومات وسلامتها[1]. كما تتحقق الجريمة بارتكاب واحد من هذه الأفعال، إضافة إلى أن الحماية الجنائية للمعطيات تتحقق فقط للمعطيات الموجودة داخل النظام، وبالتالي لا تشمل الحماية للمعلومات الموجودة خارج النظام، والتي تمت حمايتها في ظل المادة(394 مكرر2) كما سنرى لاحقا.

ج-الركن المعنوي: جريمة التلاعب في المعطيات، جريمة عمدية تتطلب قصدا جنائيا عامة يقوم على علم الجاني بأن هذه الأفعال تشكل اعتداء على سلامة المعطيات داخل النظام المعلوماتي وأنها ليست ملكا له، كما يجب أن تنصرف إرادته إلى ارتكاب هذه الأفعال، كما لا تتحقق الجريمة إلا إذا ارتكبت عن طريق الغش أي العمد. إن الفارق بين النتيجة المنصوص عليها في نص المادة(394 مكرر) وجريمة التلاعب في المعطيات باعتبارها جريمة مستقلة، يكمن في أن هذه الأخيرة تكون مقصودة بمعنى يريدها الفاعل ويقبلها على الأقل، بينما في جريمة الدخول أو البقاء لا تقع كذلك إذ لا يريدها الفاعل[2].

د- العقوبات المقررة: الحبس من ستة (6)أشهر إلى ثلاث (3)سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج .

يلاحظ أن المشرع الجزائري شدّد من العقوبة الخاصة بهذه الجريمة خلافا للجريمة المرتكبة بمفهوم نص المادة(394 مكرر 1) بسبب عنصر العمد مسايرا في ذلك المشرع الفرنسي بموجب نص المادة (2/323) من قانون العقوبات الفرنسي[3].

3- جريمة الاعتداء على المعطيات خارج النظام: كما رأينا سلفا لم يكتف المشرع الجزائري بحماية المعطيات الموجودة داخل المنظومة المعلوماتية، بل تعداها إلى حماية المعطيات الموجودة خارجها، وذلك من خلال تجريم التعامل مع هذه المعطيات الناتجة عن إحدى الجرائم المنصوص عليها في قسم المساس بأنظمة المعالجة الآلية للمعطيات، والهدف من ذلك هو الوقاية من هذه الجرائم والتخفيف من آثارها لما تمثله من خطورة بالغة على المصالح المحمية قانونا.

---

[1] رشيدة بوكر، المرجع السابق، ص268.

[2] محمد خليفة، الحماية الجنائية، المرجع السابق، ص161.

[3] ***Article 323-2 du (CPF) :***

"Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende."

أ-**الركن الشرعي:** نلاحظ أن المادة(394 مكرر2) من (ق.ع.ج)، تقابلها المادة (323-3-1) من (ق.ع.ف)[1]، وأيضا نص المادة (06) من (إ.أ.م.إ.م)، إلى جانب نص المادة (09) من (إ.ع.م.ج.ت.م) ، والتي تصطلح عليها بجرائم إساءة استخدام وسائل تقنية المعلومات[2]. حيث تنص المادة(394 مكرر2) على:" يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

ب-الركن المادي: يشتمل على صورتين:

ب1-الصورة الأولى: سنشرحها باختصار، وتتمثل في معلومات صالحة لارتكاب جريمة من الجرائم المنصوص عليها في القسم السابع مكرّر وهي:

-**التصميم *(La conception):*** هي أول عملية تتمثل في سلسلة التعامل في المعلومات وهذا العمل يقوم به عادة المتخصصون في هذا المجال كالمبرمجين ومصمّمي البرامج[3]مثل: تصميم برامج تخريبية خبيثة كالفيروسات على اختلاف أنواعها.

- **البحث *(La recherche)*:** ومعناه البحث في كيفية تصميم المعطيات وإعدادها، وليس مجرد البحث عن المعطيات لذا جاءت عبارة البحث بعد عبارة التصميم مباشرة[4].

---

[1] ***Article 323-3-1 du (CPF) :***

Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

[2] تنص المادة (09) من (إ.ع.م.ج.ت.م) على جريمة اساءة استخدام وسائل تقنية المعلومات:" إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة- كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة- حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة".

[3] محمد خليفة، الحماية الجنائية ، المرجع السابق، ص200.

[4] المرجع نفسه، ص201.

- **التجميع *(Le rassemblement)***: هو القيام بجمع أكبر عدد من المعلومات الخطيرة من الممكن أن ترتكب بها إحدى جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، كما أن المشرع استعمل لفظ الجمع بسبب أن تعدد المعلومات يرفع من درجة الخطورة، فهناك فرق بين من يحوز على معلومة وبين من يسعى لتجميعها وهو مصطلح أوسع نطاقا[1].

- **التوفير*(Mettre à disposition)***: وهو تقديم معطيات غير مشروعة يمكن أن ترتكب بها جريمة دخول أو بقاء أو جريمة تلاعب، كما تعاقب عليه المادة (06) من (إ.أ.م.إ.م) تحت عبارة:" أي أشكال للوضع تحت التصرف"، وهو يختلف عن التجميع كون هذا الأخير لا تتعدى فيه عملية حيازة المعلومات والتصرف فيها إلاّ على من يقوم بذلك، بينما في التوفير فالأشخاص الذين يحصلون على المعلومات ويتصرفون فيها تتسع دائرتهم لغيرهم مما ترتفع معه درجة الخطورة[2].

- **النشر*(La diffusion)***: ويقصد به إذاعة المعلومات محل الجريمة وتمكين الغير من الاطلاع عليها، وهي من أخطر الأفعال بسبب نقلها لعدد أكبر من الناس مما يرفع من احتمال استعمالها في الجرائم السابقة مثل: عمليات الابتزاز ضد الضحايا وذلك بطلب مبالغ مالية طائلة مقابل عدم النشر، أو بيع المعلومات في شكل أسرار إلى شركات منافسة...إلخ.

- **الاتجار*(La commercialisation)***: ويقصد به الاتجار بالمعطيات أو الأجهزة التي ترتكب بها إحدى جرائم المعلوماتية مثل: الاتجار بجهاز يحتوي برنامج معلوماتي مصمم والاتجار في بيانات المرور، أو شفرة الدخول، أو بيانات مماثلة تسمح بدخول لكل أو جزء من منظومة معلوماتية[3].

ولنبين خطورة هذه الجريمة، نشير هنا أيضا إلى قضية القرصان من ولاية باتنة التي حدثت سنة 2010، حيث تضمنت الجريمة التي قام بها كافة أشكال التعامل في معلومات غير مشروعة بمفهوم نص المادة(394 مكرر2). حيث كان يجمع المعطيات المعلوماتية الخاصة بشركة أمريكية ثم يقوم بتهديدها عن طريق نشر هذه المعلومات في مقابل حصوله على مبالغ مالية[4].

ب2–الصورة الثانية: سنتطرق إليها أيضا بصورة موجزة، وتتجلى في التعامل في معلومات متحصلة من جريمة، وتشمل أفعال:

---

1 رشيدة بوكر، المرجع السابق، ص281.

2 محمد خليفة، الحماية الجنائية، المرجع السابق، ص202.

3 هلالي عبد الإله أحمد، الجوانب الموضوعية والاجرائية لجرائم المعلومات على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة مصر، ط1، 2003، ص97.

4 أنظر: الحكم رقم:10/05272 الصادر عن محكمة باتنة بتاريخ:2010/06/01.

-**الحيازة *(La détention)***: وهي سلطة فعلية لممارسة الشخص على شيء تظهره بمظهر صاحب الحق، وتتحقق الحيازة غير المشروعة بسيطرة الحائز على المعلومات واستغلالها في ارتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كما لا تقوم الحيازة إلا بالسيطرة الإرادية التي تقترن بنية الجاني احتباس المعلومات وتوجيهها[1].

-**الإفشاء *(La révélation)***: ويقوم فيه الجاني بإفشاء المعلومات المتأتية من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بغض النظر عن الوسيلة التي بموجبها آلت إليه هذه المعلومات، وما يشكل ذلك من خطورة بحيث يقوم الجاني بتقديم هذه المعلومات لغيره الذي ليس له الحق في الاطلاع عليها، فهو لا يقصرها على نفسه فقط[2]، وهو ما يفرقه عن فعل الحيازة التي ينحصر فيها وجود المعلومات لدى الحائز دون تقديمها لشخص آخر[3].

-**النشر *(La diffusion)***: يهدف الجاني من وراء نشره للمعلومات غير المشروعة إطلاع أكبر عدد من الأشخاص عليها، وهو فعل عادة يقوم به الكراكرز أشخاص يتميزون بسعة الخبرة والإدراك الواسع للمهارات التقنية، يقومون بالتسلل إلى نظم المعالجة الآلية للمعطيات قصد الاطلاع على البيانات المخزنة فيها لسرقتها أو العبث بها أو نشرها إضرارا بخصومهم. كما لا يشترط في فعل النشر أن يتكرر لأكثر من مرة، بل يكفي لجعل الفعل قائما ارتكابه مرة واحدة، ولا يشترط في النشر ارتكابه بوسيلة معينة، ويستوي في ذلك استعمال كافة الوسائل مثل: الإنترنت، الأقراص المدمجة...إلخ[4].

-**الاستعمال *(Faire un usage)***: إذا كانت حيازة ونشر وافشاء المعلومات غير المشروعة أفعالا خطيرة، فإن الأخطر منها هو استعمالها، حيث لم يخف على المشرع أن يجرم هذا الاستعمال في حد ذاته بصفته أخطر سلوك يمكن أن يقع على المعطيات المتحصلة من جريمة مثل: استعمال شركة لمعلومات تخص شركة منافسة لها تحصلت على هذه المعلومات بعد دخول غير مشروع في النظام المعلوماتي الخاص بالشركة المنافسة[5].

يتضح لنا أن المشرع الجزائري اتجه نحو التوسع في تجريم التعامل في المعطيات التي يمكن أن تستعمل في ارتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إذ لا يقتصر الأمر على المعطيات المخزنة والمعالجة داخل النظام فقط، وإنما أيضا على المعطيات المرسلة عن طريق

---

1 رشيدة بوكر، المرجع السابق، ص286.

2 زيدان زيبحة، المرجع السابق، ص65.

3 محمد خليفة، الحماية الجنائية، المرجع السابق، ص208.

4 مصطفى محمد موسى، أساليب إجرامية، المرجع السابق، ص15 وما بعدها.

5 محمد خليفة، الحماية الجنائية، المرجع السابق، ص210.

منظومة معلوماتية. كما انفرد المشرع الجزائري عن باقي المشرعين ومنهم المشرع الفرنسي، في تجريم التعامل في معطيات متحصلة من جريمة، وهو مسلك حسن الهدف منه الوقاية من هذه الجرائم المستحدثة وضمان عدم إفلات المجرم الإلكتروني، كما أنها تندرج تحت حماية الحقوق والحريات الفردية المكفولة دستوريا بموجب نص المادة (46) من التعديل الدستوري المؤرخ في:2016/03/06 التي تنص على: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة. لا يجوز بأي شكل دون أمر معلل من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم. حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه". وهو اتجاه حسن يساير الأنظمة التشريعية الحديثة[1] في مجال حماية المعطيات ذات الطابع الشخصي[2] التي تتم معالجتها ضمن نظام المعالجة الآلية للمعطيات، خاصة في ظل توجه الجزائر نحو عصرنة منظومتها الإدارية باستخدام تكنولوجيات الإعلام والاتصال استجابة لمتطلبات الحكومة الإلكترونية.

ج–الركن المعنوي: جريمة التعامل في معلومات غير مشروعة، جريمة عمدية في صورتيها وفقا لنص المادة(394 مكرر2) حيث جاءت بلفظ"...كل من يقوم عمدا وعن طريق الغش..." تتطلب القصد الجنائي العام والقصد الجنائي الخاص. لكن هل تتطلب القصد الجنائي الخاص في صورتيها معا؟. ففي الصورة الأولى لا يكفي لقيام الجريمة توافر القصد الجنائي العام الذي يقوم على علم الجاني بتعامله في معلومات غير مشروعة يمكن أن تستعمل في ارتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إضافة إلى اتجاه إرادته في القيام بذلك وإتيان إحدى المظاهر السلوكية المجرمة، كالتصميم والنشر والاتجار...إلخ. بل لا بد من توافر أيضا القصد الجنائي الخاص المتمثل في اتجاه نية الجاني في التعامل بهذه المعلومات إلى الإعداد والتمهيد في استعمالها في ارتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. كما نشير إلى أن نص المادة(394 مكرر 2) لا يُفهم منه على أنه يشترط القصد الجنائي الخاص لتجريم هذه الأفعال وما إضافة عبارة" عن طريق الغش" إلى عبارة "عمدا" إلا لتأكيد العمدية فقط، طالما أن المشرع استعمل عبارة "عن طريق الغش" في جرائم الدخول والبقاء والتلاعب في المعطيات. أما بالنسبة

---

[1] في هذا الشأن، أصدر المجلس الأوروبي التوصية رقم:46/95 بتاريخ:1995/10/24 المتعلقة بحماية الأفراد فيما يخص معالجة المعلومات المتعلقة بهم وعملية تناقلها، حيث تتكون هذه التوصية من (34) مادة. ترى هذه التوصية أن المعلومات الفردية أصبحت لها قيمة اقتصادية مما يترتب تأمين الحماية الكافية لها خاصة إذا تم تداولها بين الدول الأعضاء، فايز الظفيري، المقال السابق، ص505.

[2] يقصد بالمعطيات ذات الطابع الشخصي: تلك المعلومات المتعلقة بأصول الشخص وبآرائه وانتماءاته السياسية أو الدينية أو النقابية وتلك المعلومات المتعلقة بأخلاقيات الشخص ذاته، غنام محمد غنام، الحماية الإدارية والجنائية للأفراد عند تجميع بياناتهم الشخصية في أجهزة الكمبيوتر، مجلة الأمن والقانون، أكاديمية شرطة دبي، الإمارات العربية المتحدة، السنة الحادية عشر، العدد2، 2003، ص90.

للصورة الثانية فهي تتطلب قصد جنائيا عاما فقط بسبب أن المعلومات متحصلة من جريمة تجعل من القصد الجنائي العام كافيا لقيامها[1].

د- **العقوبات المقررة:** الحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج.

4- إذا ارتكبت هذه الجرائم ضد الدفاع الوطني أو الهيآت والمؤسسات العامة: اتسمت السياسة الجنائية للمشرع الجزائري بخصوص جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضد الدفاع الوطني والهيآت والمؤسسات الخاضعة للقانون العام بالتشدّد، حيث أصبحت هذه المؤسسات تعتمد في تسيير شؤونها على التقنية المعلوماتية مثل: استعمال نظم معلوماتية مختلفة كقواعد البيانات...إلخ. ونظرا لأن هذه المؤسسات تمثل سيادة الدولة، فيمكن لهذه الجرائم الإخلال بأمن وسلامة الدولة ومؤسساتها خاصة في ظل توجه الجزائر وبخطوات ثابتة نحو تحقيق الحكومة الإلكترونية بغية عصرنة خدماتها والقضاء على مشكلات البيروقراطية، تجلى ذلك في إنجاز جواز السفر البيومتري وبطاقة التعريف الوطنية البيومترية، وإمكانية استخراج الوثائق الإدارية عبر الإنترنت...إلخ.

في هذا الصدد نصت المادة(394 مكرر3) من (ق.ع.ج):" تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات لخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد". من خلال نص المادة، يتضح لنا أن المشرع الجزائري حرص على توفير الحماية المطلقة لمسسة الدفاع الوطني ولمؤسسات الدولة وتوسّع في ذلك، ومنها جرائم الخيانة والتجسس التي نص عليها (ق.ع.ج) بموجب المواد من:(61 – 65) والتي تتم ضد الدولة أو مؤسساتها الدفاعية كما في حالة تسليم معلومات أو أشياء أو مستندات أو تصميمات [2] فلم يكتف المشرع بتجريم التجسس بالطرق التقليدية فقط، وإنما نص على جريمة التجسس الإلكتروني باستعمال التقنية المعلوماتية وضاعف من العقوبة عليها دون الاخلال بعقوبات أشد، وذلك وفق نص المادة(394 مكرر3) سالفة الذكر. وعليه يمكن للقاضي تطبيق العقوبات الأشد المنصوص عليها

---

1 رشيدة بوكر، المرجع السابق، ص297.

2 تنص المادة (63) من (ق.ع.ج) على:" يكون مرتكبا للخيانة ويعاقب بالإعدام كل جزائري يقوم – بتسليم معلومات أو أشياء أو مستندات أو تصميمات، يجب أن تحفظ تحت ستار من السرية لمصلحة الدفاع الوطني أو الاقتصاد الوطني إلى دولة أجنبية أو أحد عملائها على أية صورة ما وبأية وسيلة كانت –الاستحواذ بأية وسيلة كانت على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو إلى أحد عملائها –إتلاف مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد معاونة دولة أجنبية "، كما نصت المادة (64) من القانون نفسه على:" يرتكب جريمة التجسّس ويعاقب بالإعدام كل أجنبي يقوم بأحد الأفعال المنصوص عليها في الفقرات 2 و 3 و 4 من المادة 61 وفي المادتين 62 و 63" .

من المادة (60) إلى المادة(87مكرر) من (ق.ع.ج) خاصة المتعلقة بجرائم المساس بأمن الدولة ومؤسساتها ووحدتها.

وحسن فعل المشرع نظرا لما تحتويه هذا الأنظمة المعلوماتية من المعطيات الشخصية والأمنية والعسكرية، خاصة ما تعلق بمؤسسات الدفاع الوطني التي هي ذات طابع خاص بما تحتويه من معلومات سرية تمس بسلامة أمن الدولة واقتصادها، وهي مستهدفة من قبل القراصنة للحصول على المعلومات بشكل غير مشروع واستعمالها[1]، هذه الجرائم من شأنها تعطيل الأعمال الحكومية مثل: المواقع الإلكترونية الخاصة باستخدام معاملات المواطنين المقدمة لإدارة معينة[2].

5- إذا ارتكبت هذه الجرائم من طرف الشخص المعنوي: بعد أن نص المشرع الجزائري على تحميل الشخص المعنوي المسؤولية الجزائية بموجب نص المادة(18 مكرر) من (ق.ع.ج)، وفي إطار مكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وما تشكله من خطورة على المصالح المحمية قانونا. وتجاوبا مع نص المادة (12) من (إ.أ.م.إ.م)[3]، وأيضا نص المادة (20) من (إ.ع.م.ج.ت.م)[4]، نص في المادة(394 مكرر4) على:" يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم النصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

6- العقوبات التكميلية: نصت المادة(394 مكرر6) من (ق.ع.ج)على:" مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها". استثنت هذه المادة الغير حسن النية بحفظ حقوقه، ونصت على مصادرة الأجهزة كالحاسوب وملحقاته، والبرامج المصممة للاختراق وكل وسيلة

---

[1] زيدان زيبحة، المرجع السابق، ص100.

[2] عبد الله عبد الكريم عبد الله، المرجع السابق، ص28.

[3] ***Article 12 – Responsabilité des personnes morales***

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour faire en sorte que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein…", convention européenne de la cybercriminalité, Op.Cit,p.7.

[4] تنص المادة (20) من (إ.ع.م.ج.ت.م) على:" تلتزم كل دولة طرف مع مراعاة قانونها الداخلي بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيا".

مستخدمة مع إغلاق للمواقع الإلكترونية، إضافة إلى اغلاق المحلات وأماكن الاستغلال إذا تمت الجريمة بعلم صاحبها.

من خلال ما سبق ذكره، ورغم قيام المشرع بتجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، غير أنه يُطرح التساؤل الآتي: هل جرّم المشرع الجزائري كافة أشكال الاعتداء على أنظمة المعالجة الآلية للمعطيات؟. هذا ما سنجيب عنه في الفرع الموالي:

الفرع الثاني: مدى كفاية القانون:04-15 لتجريم كافة أشكال الاعتداء على أنظمة المعالجة الآلية للمعطيات:

تعتبر المنظومة المعلوماتية هدفا دائما للقراصنة نظرا لما تحتويه من معطيات هامة تتعلق بالأشخاص المعنوية أو الطبيعية، قصد استعمالها لأغراض متعددة عادة ما تكون بقصد تحقيق عوائد مالية أو الابتزاز أو التهديد كما رأينا سابقا. وعلى الرغم من أن المشرع الجزائري كان سبّاقا لتجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم:04-15 المعدل والمتمم لقانون العقوبات، من هنا يطرح التساؤل: هل أحاط المشرع الجزائري بكافة أشكال الاعتداءات على المنظومة المعلوماتية؟. وقبل الإجابة لا بد من أن نتعرف أولا إلى بعض أشكال الاعتداءات الأخرى على أنظمة المعالجة الآلية للمعطيات، ثم نتطرق ثانيا إلى مدى كفاية القانون رقم:04-15 لتجريمها.

أولا: أشكال الاعتداء الأخرى على أنظمة المعالجة الآلية للمعطيات: سنتطرق للبعض منها كما يأتي:

1- جرائم إفساد سير الأنظمة: يقصد بإعاقة سير العمل في النظام المعلوماتي:" القيام بأي فعل يسبب تباطؤ عمل نظام المعالجة الآلية للمعطيات أو إرباكه، مما يؤدي إلى تغيّر في حالة عمل النظام على نحو يصيبه بالشلل المؤقت، وذلك باستعمال البرامج الخبيثة كالفيروسات والقنابل المنطقية ...إلخ"[1]، كما يتم أيضا إفساد عمل النظام بواسطة تعديل البرنامج الأصلي أو إدخال برنامج آخر كما قد يقع الاعتداء على الشبكات التي تغذي النظام المعلوماتي دون دخوله[2]، تشكل هذه الجريمة خطرا كبيرا على النظام المعلوماتي بما يتسبب في خسارة كبيرة للمؤسسات والشركات المصنعة[3]

---

1 محمد أمين الشوابكة، المرجع السابق، ص223، راجع أيضا، *Alain Bensoussan ,Internet, Op.Cit,p.200.*

2 هلالي عبد الإله أحمد، الجوانب الموضوعية، المرجع السابق، ص92.

3 حادثة شركة أوميغا *(Omega)* : تتلخص وقائع هذه القضية في قيام مصمم ومبرمج شبكات كمبيوتر ورئيس سابق لشركة *(Omega)* من مدينة *(Delaware)* الأمريكية ويدعى: *(Timothy Allen Lioyd)* يبلغ من العمر 35 عاما، بإطلاق قنبلة إلكترونية *(E-bombs)* سنة 1996 بعد عشرون يوما من فصله من عمله، حيث تسببت في أضرار بالغة واستطاعت أن تلغي كافة== ==التصاميم وبرامج الإنتاج لأحد كبريات مصانع التقنية العالية في نيوجرسي والمرتبطة والمؤثرة على نظم تحكم معلوماتية مستخدمة في

اعتبر المشرع الفرنسي تجريم إفساد سير الأنظمة أولوية ملحة لاكتمال منظومة مكافحة الجريمة الإلكترونية[1]، حيث تناول الأحكام المتعلقة بجرائم الإتلاف والتخريب والتعييب أو التهديد بشيء من ذلك بموجب المواد من (1/323) إلى (7/323) من (ق.ع.ف). يمكن القول أن هذه النصوص تعاقب على مختلف صور الإتلاف التي يمكن أن تفسد سير عمل النظام المعلوماتي[2]، فقد تكون وسيلة التعطيل مادية كما لو وقع على الأجهزة عنف أو تخريب أو قطع وسائل الاتصال، وقد تتحقق بوسائل معنوية مثل: إدخال فيروس في نظام التشغيل[3]، ولاسيما نص المادة (1/323) (ق.ع.ف) التي تعاقب على أفعال المحو والتعديل التي تؤدي إلى إفساد سير النظام[4]. ولكنه بالمقابل لم يجرم فعل الإعراض أو الإلتقاط بموجب نص خاص.

وفي السياق نفسه، لم ينص المشرع الجزائري على فعل الاعتراض أو الالتقاط أو تحريف سير النظام المعلوماتي بموجب نص خاص شأنه في ذلك شأن المشرع الفرنسي، واكتفى بنص المادة (394مكرر/3) التي تنص على: "...وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة...". ويطرح هنا التساؤل عن سبب عدم إفراده لنص خاص لتجريم هذه الأفعال، وخاصة أنها جرائم أساسية ترتكب ضد الأنظمة المعلوماتية؟، وهل يعتبر نص المادة(394 مكرر) كافيا لذلك؟، ربما يرجع سبب ذلك إلى التشابه الموجود بين هذه الجريمة وجريمة التلاعب بالمعلومات مما يحول دون التمييز بينهما في كثير من الأحيان، وذلك بسبب أن الأفعال التي تتضمنها جريمة التلاعب تؤدي هي الأخرى إلى إعاقة النظام وإفساده[5]. في هذه الجرائم يقوم الجاني باعتراض أو التقاط المعلومات التي يتم نقلها إلكترونيا باستعمال وسائل فنية تمكن من الحصول على محتو الاتصالات سواء عن طريق الدخول بشكل مباشر إلى النظام المعلوماتي أو بطريق غير مباشر

وكالة الفضاء الأمريكية *(NASA)* والبحرية الأمريكية، ملحقا خسائر بلغت 10 مليون دولار. تعتبر هذه الحادثة مثالا حيا على مخاطر جرائم التخريب في بيئة الكمبيوتر، تم اعتقاله في:1998/02/17 ، راجع، يوسف يوسف حسن، المرجع السابق، ص ص53-54.

[1] *André Lucas et Autres, Op.Cit,p.679.*

[2] *jean Larguier et Autres, Op.Cit,p.242.*

[3] أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني–دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، ط1، 2006 ص118.

[4] ***Article 323-1 du (CPF) :***

"Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende."

[5] محمد خليفة، الحماية الجنائية، المرجع السابق، ص175.

باستعمال أجهزة التنصت وتسجيل الأصوات[1]، وعليه يقوم الجاني بخلق نظام وسيط وهمي بحيث يكون على المستخدم أن يمر من خلاله ويزود النظام بمعلومات حسّاسة بشكل طوعي[2].

من جانب آخر يختلف اعتراض الرسائل التي ترسل عن طريق حاسوبين على شبكة مغلقة أو عن طريق الإنترنت عن جريمة الدخول والبقاء، بسبب أن الاعتراض يمثل نوعا من التلصّص على فحوى الرسائل المرسلة بين جهازين من الأجهزة[3]. في هذا الشأن أوصى المجلس الأوروبي بضرورة إفراد نص خاص لتجريم فعل الاعتراض الذي يتم من وإلى نظام المعالجة الآلية للمعطيات أو شبكة الاتصالات[4]. من جهة أخرى أورد المشرع الجزائري تعريفا للاتصالات الإلكترونية بموجب نص المادة (02/و) من القانون رقم:09-04 السابق ذكره على أنها:" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية...". كما عرف لنا أيضا المشرع الاتصالات الإلكترونية بموجب نص المادة (05) من المرسوم الرئاسي رقم:15-261 المؤرخ في:10/08/ 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي تنص على: "يقصد في مفهوم هذا المرسوم ما يأتي: "الاتصالات الإلكترونية: كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية، بما في ذلك وسائل الهاتف الثابت والنقال..."[5].

وعليه وسّع المشرع من مفهوم الاتصالات الإلكترونية ليشمل كل وسائل نقل المعلومات التي تتم بطريقة إلكترونية كالهاتف الثابت والنقال وجهاز الفاكس...إلخ، وسواء تمت الاتصالات داخل النظام نفسه أو بين مجموعة أنظمة متصلة فيما بينما. وكما قلنا سابقا أن نص المادة (394مكرر) لا يتضمن تجريم أفعال إفساد سير الأنظمة المعلوماتية، فكان على المشرع النص على تجريمها بموجب

---

[1] رشيدة بوكر، المرجع السابق، ص207.

[2] يونس عرب، البنوك الخلوية، التجارة الخلوية، المعطيات الخلوية، ثورة جديدة تنبئ بانطلاق عصر ما بعد المعلومات، بحث منشور على الموقع الآتي: *http://www.abhatoo.net.ma* ، تاريخ الاطلاع:2016/10/01 على الساعة:17:01، ص26.

[3] فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه، جامعة الجزائر1، كلية الحقوق، 2011 ص195.

[4] ***Titre 5- Collection en temps réel de donnée informatique :***

"les articles 20 et 21 prévoient la collecte en temps réel de donnée relative au trafic et l'interception en temps réel de donnée relative au contenue associée à des communications précise transmise au moyen d'un système informatique …"conseil de l'Europe, comité des ministères, Recommandation n : R (89)9 sur la criminalité en relation avec l'ordinateur, Strasbourg, 1989, p53.

[5] المرسوم الرئاسي رقم:15-261 المؤرخ في:10/08/ 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (ج. ر) رقم:53 المؤرخة في:2015/10/08 ، ص ص16-21.

نص خاص في ظل انتشار أنظمة الاتصال اللاسلكية كنظام الواي فاي*(WIFI)* والتقنية الجديدة *(LIFI)*[1] الذي يمكن من خلالها اعتراض المعلومات بسهولة. هذا ما نأمل أن يفعله المشرع حينما يحول نصوص (إ.ع.م.ج.ت.م) –التي تنص على جريمة الاعتراض غير المشروع للبيانات– إلى نصوص تشريعية داخلية.

2- جريمة سرقة وقت النظام المعلوماتي: تتداخل وتتشابه جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، مع مفهوم سرقة وقت نظام المعالجة الآلية الذي مفاده: "عمل الجاني على تشغيل النظام أثناء وقت فراغه، سواء لحسابه الشخصي أو لمنفعة شخص آخر خلال مدة معينة من الزمن، وذلك بدون علم صاحب الجهاز"[2]. كما يعني أيضا:" تطبيقا للاستخدام بطريق التحايل"[3]. فيمكن أن يقوم شخص بهذه الأفعال سواء كانت له صلاحية الدخول للنظام أم لا، وتتم سرقة –منفعة–وقت النظام المعلوماتي بالاستخدام غير المشروع للأنظمة المعلوماتية، وسرقة الخدمات المعلوماتية *(Theft of services)* أو سرقة الوقت *(Time Theft)*، وهي واسعة الانتشار في مجال المعلوماتية مثل: استخدام أرقام حسابات الشركات أو التلاعب ببيانات الحاسوب لمعرفة الوقت الفعلي لدفع الأجرة أو لمعرفة زبائن الشركة أو الخدمات التي تقدمها[4]، وهذا الاستخدام غير المشروع بالتأكيد مرفوض من جانب صاحب الحق[5]. إلا أنه يمكن تسجيل أن غالبية حالات

---

[1] نظام الواي فاي *(wifi)*: *(Wi)*هي اختصار لـ *(Wireless)* ، و*(Fi)* هو مقطع ليس له معنى أُضيف للتناغم فقط، وهو مصطلح يستخدم لتعريف تقنيات الاتصال اللاسلكي، وهي التقنية التي تقوم عليها معظم الشبكات اللاسلكية *(WLAN)* اليوم، فهي تستخدم موجات الراديو لتبادل المعلومات بدلاً من الأسلاك والكوابل. كما أنها قادرة على اختراق الجدران والحواجز، وذات سرعة عالية في نقل واستقبال البيانات تصل إلى 54 .Mbps .ويتوقع لتكنولوجيا واى فاى أن تتطور وأن تتغير كما تتغير معظم التطبيقات التكنولوجية الأخرى. وقد ظهرت في الأفق تقنية جديدة تسمي *(LIFI)*. تستعمل مصابيح ضوئيّة شبكيّة تسمى: *(Led)*، يتم نشر وانشاء الاتصال ضوئياً عن طريق مصابيح خاصّة تقوم بنشر الإشارة ضمن الضوء الصادر عنها، كما أنها تقلّل من استهلاك الطاقة وتدوم مدى الحياة، وإنّ هذه المصابيح تبدو الحل الأنسب الذي لا يمكن الاستغناء عنه في تقليل كمية الـ *(CO2)* المطروحة على المدى الطويل. يبلغ معدل نقل البيانات أسرع بعشرة مرّات مقارنة بتقنية *(WIFI)* يصل إلي 1 *(Giga Bytes)* في الثانية، مما سيطرح مشكلة جديدة بخصوص جريمة اعتراض والتقاط الرسائل عبر الوسائل الإلكترونية، ومنها نظم المعالجة الآلية للمعطيات،- *Myriam Quéméner et Joel Ferry,Op.Cit,pp.15-16.*،أكثر تفاصيل حول الموضوع، راجع أيضا الرابط الآتي:

https://ar.wikipedia.org/wiki/%D9%88%D8%A7%D9%8A-%D9%81%D8%A7%D9%8A،تاريخ الاطلاع:2015/12/03 على الساعة:11:37.

[2] جميل عبد الباقي الصغير، الجرائم الناشئة، المرجع السابق، ص64.

[3] هدى حامد قشقوش، المرجع السابق، ص84.

[4] محمد أمين الشوابكة، المرجع السابق، ص171.

[5] هدى حامد قشقوش، المرجع السابق، ص84.

سرقة وقت النظام المعلوماتي ليس لها هدف إجرامي، فقد يلجأ إليها بعض الأشخاص لفعل الخير كتحرير بطاقات مخصصة للأعمال الخيرية أو لنسخ ألعاب الفيديو لاستعمالهم الشخصي[1].

من جانبه لم يفرد المشرع الجزائري نصا خاصا لتجريم هذا الفعل مما يؤدي إلى اللاّعقاب في صورة استعمال غير مصرح لوقت نظام المعالجة الآلية للمعطيات[2]. إلا أن هناك من يرى أن النصوص الخاصة بجريمة الدخول أو البقاء غير المصرح به يمكن تطبيقها على فعل سرقة وقت نظام المعالجة الآلية على أساس أن هذا الاستعمال مرفوض من صاحب النظام[3]، وربما هذا ما جعل المشرع الجزائري لم يفرد هذه المسألة بنص خاص. إن هذا الفعل وإن كان يتداخل كثيرا مع فعل الدخول غير المصرح به، إلا أن هناك فرقا بينهما على أساس أن جريمة الدخول غير المشروع تتم بمجرد الدخول للنظام بغض النظر عن الانتفاع، بينما يقوم فعل سرقة وقت النظام على استخدامه بغير وجه حق.

ثانيا: مدى كفاية نصوص القانون 04-15 لتجريمها: يعد تدخل المشرع الجزائري في مجال مكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات قفزة نوعية، وذلك بتجسيده معظم أحكام (إ.أ.م.إ.م)، إضافة إلى بعض أحكام (إ.ع.م.ج.ت.م)، وذلك من خلال:

-تجريم أفعال الدخول والبقاء غير المشروع داخل النظام المعلوماتي وتشديد العقوبة عليه إذا ترتب عن ذلك حذف أو تغيير معطيات المنظومة المعلوماتية، أو تخريب نظام اشتغال المنظومة المعلوماتية.

-التوسّع في مفهوم الدخول غير المشروع ليشمل فعل الدخول والبقاء قصد بيان السلوك المجرم كتحديد الأشخاص المخول لهم بالدخول وحالات الدخول غير المرخص بها.

- تجريم أفعال التلاعب في معطيات المنظومة المعلوماتية مثل: إدخال أو إزالة أو تعديل معطيات المنظومة ما لم يكن مصرحا بذلك. وهذا بقصد ضمان سريتها وسلامتها ووفرتها. كما وسّع المشرع من نطاق الحماية لتشمل كافة أنواع المعلومات وجميع وسائل التلاعب بها.

-التوسّع في محل الحماية ليشمل فعل الدخول والبقاء غير المشروعين في كل المنظومة المعلوماتية أو جزء منها.

---

[1] محمد سامي الشوا، المرجع السابق، ص170.

[2] رشيدة بوكر، المرجع السابق، ص222.

[3] هدى حامد قشقوش، المرجع السابق، ص84.

-حصر السلوك المجرم في جريمة التعامل في معلومات غير مشروعة في المعطيات المخزنة أو المعالجة أو المرسلة فقط بواسطة منظومة معلوماتية، في حين تتوسع في ذلك بعض التشريعات المقارنة ومنها المشرع الفرنسي.

-تجريم أفعال الاعتداء على سلامة المعطيات خارج المنظومة المعلوماتية عن طريق الحيازة والإفشاء والنشر والاستعمال...إلخ.

-عدم اشتراط المشرع الجزائري لقيام الجريمة وجود نظام حماية للمنظومة المعلوماتية.

-مضاعفة العقوبة تبعا لصفة المجنى عليه، وذلك إذا مست هذه الجرائم الدفاع الوطني أو الهيآت والمؤسسات الخاضعة للقانون العام، وهو مسلك انفرد به المشرع الجزائري.

-تبنى المشرع مبدأ مسؤولية الشخص المعنوي الذي يرتكب هذه الجرائم وشدّد من العقوبة عليها.

- توسيع نطاق العقوبة لقطع دابر الجريمة، وذلك بتجريم الشروع والاتفاق الجنائي.

-النص على العقوبات التكميلية مثل: المصادرة والغلق في حالة الحكم بالعقوبة السالبة للحرية في جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

لقد وفق المشرع الجزائري في سياسته الجنائية، الهادفة إلى تحقيق أمن المعلومات[1] باتخاذه التدابير اللازمة لحماية سرية وسلامة ووفرة وإتاحة المعلومات[2]، خاصة في ظل انتشار تقنية المعلومات وتوجه الجزائر إلى اتباع أسلوب الحكومة الإلكترونية، وما تفرضه هذه الأخيرة من تحديات تقنية خاصة ما تعلق بأمن المعطيات التي هي في غاية الحساسية بالنسبة للدولة والأفراد على حد

---

[1] يقصد بمصطلح :"أمن المعلومات":" محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة" ، وهو هدف تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت)، راجع، يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها، بحث منشور على الموقع الآتي: *http://www.abhatoo.net.ma*، تاريخ الاطلاع:2016/10/01 على الساعة: 17:42، ص1.

[2] تتمثل عناصر أمن المعلومات في:

-السرية أو الموثوقية *(CONFIDENTIALITY)* : وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.

-التكاملية وسلامة المحتوى *(INTEGRITY)*: التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

-استمرارية توفر المعلومات أو إلخدمة *(AVAILABILITY):* التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وإن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها .

-عدم إنكار التصرف المرتبط بالمعلومات ممن قام به (*Non-repudiation*): ويقصد به ضمان عدم إنكار الشخص الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من طرف شخص ما في وقت معين، المرجع نفسه، ص ص2-3 .

سواء. حيث استطاعت نصوص القانون رقم:04-15 المعدل والمتمم استيعاب الصور المتطورة للجرائم التقليدية إلى حد كبير، والتي تكون فيها المنظومة المعلوماتية وسيلة لارتكابها بسبب الطبيعة التقنية الخاصة لهذه الجرائم فهي تتم في بيئة افتراضية يباشر فيها المجرم الإلكتروني نشاطه في صورة نبضات وإشارات كهرومغناطيسية، مما يخلق صعوبات جمة للأجهزة القضائية المختصة في مكافحتها سواء على مستوى اكتشافها، أو على مستوى ملاحقة مرتكبيها. كما نستخلص أيضا من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية وجود تدرج داخل النظام العقابي، بهدف تحديد الخطورة الإجرامية لهذه الأفعال.

غير أننا نسجل بعض النقائص المتمثلة في إغفال المشرع النص على بعض الجرائم والتي تناولناها سابقا، رغم أنها جرائم أساسية تمس بأنظمة المعالجة الآلية للمعطيات وهي:

- جريمة الاعتداء العمدي على سلامة وسير نظم المعالجة الآلية للمعطيات واكتفى بنصوص المواد(394 مكرر إلى 394 مكرر2).
- جريمة سرقة وقت النظام المعلوماتي.
- جريمة التنصت على النظام المعلوماتي.
- تجريم كافة أشكال الإرهاب الإلكتروني الذي أصبح لا يستغنى عن استعمال تقنية المعلومات، حيث اقتصر المشرع على جريمة الإشادة بالأفعال الإرهابية التي تتم بأي وسيلة كانت كما سنوضحه في المطلب الموالي.

وعليه تعتبر هذه الجرائم شكلا آخرا من أشكال الاعتداء على المنظومة المعلوماتية، لذا ندعو المشرع إلى تدارك هذا النقص التشريعي خاصة بعد تصديق الجزائر على نصوص(إ.ع.م.ج.ت.م) وذلك بتحويل الاتفاقية إلى نصوص تشريعية داخلية بما يحقق تكامل وفعالية للسياسة الجنائية للمشرع الجزائري في شقيّها الموضوعي والإجرائي في مكافحة هذا النوع المستحدث من الجرائم الذي يمتاز بالتطور المستمر تبعا لتطور تقنية المعلومات.

المطلب الثالث: الإرهاب الإلكتروني

أدّت الثورة التكنولوجية في مجال تقنية المعلومات إلى بروز أشكال جديدة من الإجرام الإلكتروني على غرار مصطلح الإرهاب الإلكتروني(الإرهاب السيبيري)، حيث يتميز عن الإرهاب التقليدي بالطريقة العصرية المتمثلة في استخدام المواد المعلوماتية والوسائل الإليكترونية التي وفرتها تقنية عصر المعلومات، مما زاد من خطورته سواء من حيث تسهيل الاتصال بين الجماعات الإرهابية وتنسيق عملياتها والإشهار لها والإشادة بها، أو من حيث المساعدة على ابتكار أساليب وطرائق

إجرامية متقدمة[1]. ومع انتشار الوسائل التكنولوجية الحديثة كشبكة الإنترنت، فإن مهمة بعث الرعب عن طريق خطابات أو أفكار محددة غدت أكثر سهولة ويسرا[2]، مما جعل المجموعة الدولية تتكاتف قاطبة للتنسيق فيما بينها لمحاربة هذه الظاهرة على أساس أن الإرهاب يمس الجميع وليس له حدود. سنتطرق إلى مفهوم الإرهاب الإلكتروني في (الفرع الأول)، ثم نتناول أشكاله في (الفرع الثاني).

الفرع الأول: مفهوم الإرهاب الإلكتروني:

ينطلق مفهوم الإرهاب الإلكتروني من تحديد مفهوم الإرهاب، وفي هذا الشأن لم يتفق الفقهاء حتى الآن على وضع تعريف ثابت وجامع له بسبب تعارض مفهومه بين الدول نتيجة التباين في المصالح، فما يعد إرهابا عند دولة ما ليس بالضرورة إرهابا عند أخرى.

في هذا الصدد، عرفت المادة (2/01) من الاتفاقية العربية لمكافحة الإرهاب على أنه:" كل فعل من أفعال العنف والتهديد أيا كانت بواعثه أو أغراضه، يقع تنفيذ المشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس أو تخويفهم أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو أحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر"[3]. أو هو:" الفعل الإجرامي المرتكب من قبل أفراد أو جماعات منظمة أو دول والتي تستخدم فيها وسائل من شأنها إدخال الرعب أو الفزع في قلوب مجموعة من الأفراد أو كافة أفراد المجتمع بدون تمييز بهدف إحداث خطر عام أو ضرر جسيم كوسيلة للوصول إلى أهداف إيديولوجية أو سياسية أو دينية أو عنصرية معينة"[4].

وبمصادقة الجزائر على هذه الاتفاقية بتاريخ:1999/03/09 ،عرف المشرع الجزائري الإرهاب بالأفعال الإرهابية أو التخريبية في القسم الرابع مكرر من قانون العقوبات تحت عنوان:" الجرائم الموصوفة بأفعال إرهابية أو تخريبية"، حيث نصت المادة (87مكرر) من (ق.ع.ج)على: "يعتبر فعلا إرهابيا أو تخريبيا في مفهوم هذا الأمر، كل فعل يستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يأتي : بث الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء المعنوي والجسدي على الأشخاص أو

---

[1] *Myriam Quéméner et Yves Charpenel,Op.Cit,p.125.*

[2] يوسف كوران، المرجع السابق، ص54.

[3] أنظر: نصوص الاتفاقية العربية لمكافحة الإرهاب، منشورة على الموقع الرسمي لجامعة الدول العربية على الرابط الآتي: *http://www.lasportal.org/ar/legalnetwork/Pages/agreements_details.aspx?RID=68*،تاريخ الاطلاع:2015/12/08 على الساعة:11:33.

[4] يوسف كوران، المرجع السابق، ص ص22-23.

تعريض حياتهم أو أمنهم للخطر أو المس بممتلكاتهم... عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام..."

وعليه وفي ظل توجه الدولة نحو الحكومة الإلكترونية، يمكن أن تكون الأنظمة المعلوماتية والمعطيات المخزنة بها محلا لجريمة الإرهاب الإلكتروني، بحيث يمكن شن هجوم إرهابي إلكتروني على البنية التحتية للشبكة المعلوماتية بقصد تدميرها وإلحاق الضرر بالسير العادي لمرافق الدولة بحيث يتمثل الركن المادي في القيام بأي فعل من شأنه الاعتداء على المنظومة المعلوماتية أو المعطيات المخزنة فيها بما يحقق تهديد أمن الدولة ومؤسساتها. ومنه يمكن تعريف الارهاب الإلكتروني على أنه:" استعمال تقنية المعلومات من طرف منظمات إجرامية أو أشخاص لأجل ممارسة ضغوطات لإرهاب الخصوم"[1].

وما يهمنا في هذا القسم الرابع مكرر هو الإشارة إلى جريمة الإشادة بالأفعال الإرهابية بموجب نص المادة (87مكرر4) التي تنص على:" يعاقب بالسجن المؤقت من خمسة (5) سنوات إلى عشر (10) سنوات وبغرامة مالية من 100.000دج إلى 500.000 دج، كل من يشيد بالأفعال المذكورة في المادة (87مكرر) أعلاه أو يشجعها أو يمولها بأية وسيلة كانت". حيث يقوم الركن المادي لهذه الجريمة على الأفعال الآتية:

- الترويج للجرائم الإرهابية(الإشادة والتشجيع): يتمثل فعل الإشادة في التنويه بالأفعال الإرهابية والثناء عليها، أما فعل التشجيع يعني الحث وبعث الرغبة في القيام بالأعمال الإرهابية، كإلقاء الخطب والكتابة والرسم...إلخ، أو ما يسمى في كلتا الحالتين بالتمويل المعنوي.

- تمويل المنظمات الإرهابية: ويقصد التمويل المادي كتوفير الأموال في صورتها النقدية أو العينية، كما يجب أن يكون النشاط الجرمي وفقا لمقتضيات المادة (87مكرر) سالفة الذكر.

✓ الوسيلة المستعملة: تتعدد هذه الوسائل، مثل: التلفزيون، والفيديو، الجرائد والمجلات...إلخ كما يحمل فعل الترويج معنى العلانية.

فبالرجوع إلى نص المادة استعمل المشرع عبارة:"... بأية وسيلة كانت" رغبة منه في توسيع مفهومها واحتواء جميع الوسائل التقنية التي ستظهر مستقبلا، فنظريا يمكن تطبيق نص المادة على أفعال الإشادة التي تتم باستعمال تكنولوجيات الإعلام والاتصال الحديثة كالهاتف النقال وشبكة الإنترنت...إلخ. بالمقابل تتعدد أشكال الإرهاب الإلكتروني –الذي سنتطرق إليه في الفرع الموالي–بما يخلق صعوبات في تكييف الجريمة واحتواء نص هذه المادة لكافة أشكاله، ومنها أفعال ترويع وتخويف وبث الرعب بين السكان باستعمال تقنية المعلومات خاصة شبكة الإنترنت وهو ما يوافق

[1] *Ali EL AZZOUZI, Op.Cit,p.76.*

نص المادة (87مكرر/1) التي تنص على:" بث الرعب في أوساط السكان..."، فالمشرع لم يوضح لنا الوسيلة المستعملة في ذلك. مما يجعل هذا النص غير قادر على استيعاب كافة أشكال الإجرام الإلكتروني، بما يفرض على المشرع الجزائري تعديل هذه المادة لتصبح:" بأي وسيلة تقنية أو معلوماتية كانت" أو التجريم بموجب نص جديد تطبيقا لنص المادة (15) من (إ.ع.م.ج.ت.م) المتعلقة بجرائم الإرهاب والمرتكبة بواسطة تقنية المعلومات، حيث تنص على:" نشر أفكار ومبادئ جماعات إرهابية والدعوة لها – تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية – نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية– نشر النعرات والفتن والاعتداء على الأديان والمعتقدات".

وخلاصة القول ورغم تضمن قانون العقوبات للأفعال الموصوفة بالإرهاب، إضافة إلى قوانين أخرى كالقانون رقم:01-50 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما والقانون رقم:09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، إلا أنها لم تتضمن النص صراحة على تجريم الإرهاب الإلكتروني في أشكاله التي تناولناها آنفا، مع إمكانية تدخل المشرع لتطويع النصوص الحالية في مجال مكافحة الجرائم الإلكترونية أو استحداث نصوص جديدة تطبق على هذا النوع من الجرائم، خاصة ما تعلق بالمساس بأنظمة المعالجة الآلية للمعطيات وشبكة الإنترنت مثل: المواقع الإلكترونية التي توفر الدعاية للأعمال الإرهابية وكيفية استخدام الأسلحة والتدريب على صنع القنابل والمتفجرات، مع فرض عقوبات مشددة على مرتكبيها.

وفي انتظار قيام المشرع بذلك، بادرت وزارة الداخلية والجماعات المحلية ووزارة الدفاع الوطني باستحداث لجنة أمنية مشتركة متخصصة في مكافحة الإرهاب الإلكتروني وتعقّب المنتديات الجهادية على خلفية تزايد نشاط شبكات تجنيد تم تفكيكها من قبل وحدات الدرك الوطني والشرطة والجيش في 16 ولاية. وبينت تحريات أمنية دقيقة أن كل تلك الشبكات استخدمت مواقع التواصل الاجتماعي وحثّت عناصرها على ولوج منتديات جهادية ومواقع تزرع أفكارا متطرفة.

---

[1] في هذا الصدد، خوّل المشرع الجزائري بموجب المادة (04) من القانون رقم:09-04 لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من جرائم الإعلام والاتصال المنصوص عليها بموجب المادة (13) من القانون نفسه، حق الرقابة الإلكترونية على الأفعال ذات الصلة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة، أو الاعتداء على منظومة معلوماتية بما يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة، وما يلاحظ تضمن هذا النص على الرقابة الإلكترونية ولكن كفعل وقائي من هذه الجرائم ولم ينص صراحة على جرائم الإرهاب الإلكتروني بصفة مستقلة رغم تعدد أشكاله.

الفرع الثاني: أشكال الإرهاب الإلكتروني:

يستخدم الإرهاب الإليكتروني الامكانات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، في تخويف وترويع الآخرين وإلحاق الضرر بهم أو تهديدهم. سنتطرق بإيجاز إلى أهما وأكثرها خطورة فيما يلي:

أولا: نشر وتبادل المعلومات الإرهابية من خلال الإنترنت: ويتم ذلك من خلال الشبكة المعلوماتية التي توفر كما هائلا من المعلومات ذات أهمية بالغة للمنظمات والجماعات الإرهابية حيث تستطيع نشر أفكارها المتطرفة والسيطرة على وجدان الأفراد بغية تجنيدهم للقيام بأفعال إرهابية. كما يستخدم الإرهابيون الإنترنت في التنسيق فيما بينهم والتخطيط للعمليات الإرهابية، مستفيدين من عنصر التخفي وباستعمال تقنيات التشفير[1]، كما يعتبر البريد الإلكتروني أداة فعّالة في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم ، بل إن كثيرا من العمليات الإرهابية وقعت نتيجة لاستخدام البريد الإليكتروني في تبادل المعلومات بين القائمين بالعمليات الإرهابية والمخططين لها، بعيدا عن الملاحقة الأمنية التي تأتي في غالب الأحيان متأخرة[2].

ثانيا: إنشاء المواقع الإرهابية الإلكترونية: يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة الإنترنت للدعوة لأفكارهم المتطرفة، ولإعطاء التعليمات وللتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية، فقد أنشأت مواقع إرهابية إلكترونية لبيان كيفية صناعة القنابل والمتفجرات، والأسلحة الكيماوية الفتاكة، ولشرح طرق اختراق البريد

---

[1] التشفير*(ENCRYPTION)*:عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفَّرَة. ومن المعلوم أن الإنترنت تشكِّل في هذه الأيام الوسط الأضخم لنقل المعلومات. ومن بينها المعلومات الحساسة (مثل الحركات المالية) بصيغة مشفَّرة إن أُريدَ الحفاظ على سلامتها وتأمينها من عبث قراصنة المعلوماتية. وتُستخدَم المفاتيح في تشفير *(encryptions)* الرسالة وفك تشفيرها *(décryptions)* حيث تستنِد هذه المفاتيح إلى صيغ رياضية معقَّدة (خوارزميات). وتعتمد قوة وفعالية التشفير على عاملين أساسيين: الخوارزمية، وطول المفتاح مقدَّرا بالبايت*(bits)* ومن ناحية أخرى، فإن فك التشفير هو عملية إعادة تحويل البيانات إلى صيغتها الأصلية، وذلك باستخدام المفتاح المناسب لفك الشيفرة، حسن بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص375، راجع أيضا عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، ط1، 2003، ص ص49-51 ، وأيضا، *Myriam Quéméner et Yves Charpenel,Op.Cit,p.81*

[2] جميل عبد الباقي الصغير، مدى كفاية نصوص قانون العقوبات والإجراءات الجنائي لمواجهة الإرهاب عبر الإنترنت، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية،2008، ص12.

الإلكتروني، وكيفية اختراق وتدمير المواقع الإلكترونية، والدخول إلى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات...إلخ[1].

ثالثا: تدمير المواقع الإلكترونية والأنظمة المعلوماتية: تهدف التنظيمات الإرهابية من خلال هجمات إلكترونية إلى تدمير البنية التحتية لمرافق الدولة، كما تستهدف أيضا تدمير الأهداف العسكرية والسياسية والاقتصادية، والمصارف والأسواق المالية، بحيث يلحق ضررا كبيرا بها مما يؤدي إلى توقف القطاعات والمرافق الحيوية عن العمل، خاصة في ظل توجه أغلب الدول إلى اعتماد أسلوب الحكومة الإلكترونية في تسيير شؤون الدولة والمواطنين. ويقصد بالتدمير في هذا الصدد الدخول غير المشروع على نقطة ارتباط أساسية أو مجموعة، *(Server- PC)* أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام آلي بهدف تخريب نقطة الاتصال أو النظام[2].

رابعا: التجسس الإلكتروني: يقوم الإرهابيون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عمليات التجسس الإرهابي في عصر المعلومات ثلاثة أهداف رئيسة هي: التجسس العسكري، والتجسس الشخصي، والتجسس التجاري ففي التجسس العسكري مثلا تحاول المنظمات الإرهابية اختراق حواسيب وزارات الدفاع للدول المعنية قصد الحصول على معلومات عسكرية مثل: عدد القوات ونوعية تسليحها وأماكن تواجدها...إلخ، كما تتم عملية التجسس الإلكتروني بعدة طرق، منها استخدام برامج التجسّس مثل برنامج حصان طروادة وبرامج تسجيل المفاتيح والأبواب الخلفية وبرامج مراقبة الإنترنت، وغرف الدردشة...إلخ[3]، ومن أشهر الطرق شيوعا استعمال وسيلة البريد الإلكتروني *(E-mail)*حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر، أو باستعمال أسلوب إخفاء المعلومات داخل المعلومات ويتلخص هذا الأسلوب في لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة بداخل معلومات أخرى عادية داخل الحاسوب ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها، وبذلك لا يشك أحد في أن هناك معلومات حساسة يتم تهريبها[4].

بعدما عرفنا الجرائم الإلكترونية الماسة بأنظمة المعالجة الآلية للمعطيات، يُثار التساؤل الآتي: هل هناك جرائم إلكترونية أخرى نص عليها المشرع الجزائري خارج الجرائم سالفة الذكر؟.

---

[1] عبدالله بن عبدالعزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في المدة من 2 – 4 يونيو 2008، متوفر على الرابط الآتي: *http://www.shaimaaatalla.com/vb/showthread.php?t=3937*، تاريخ الاطلاع:2015/12/08 على الساعة:17:08

[2] جميل عبد الباقي الصغير، مدى كفاية، المرجع السابق، ص15.

[3] حسين بن سعيد الغافري، السياسة الجنائية، المرجع السابق ، ص ص380 -393.

[4] جميل عبد الباقي الصغير، مدى كفاية، المرجع السابق، ص17، راجع أيضا، محمد أمين الرومي، المرجع السابق، ص136.

المطلب الرابع: صور المساس بحرمة الحياة الخاصة باستعمال الوسائل التقنية

لا شك بأن الحق في الخصوصية *(Privacy)* معترف به للشخص الطبيعي بصفته الإنسانية كأصل عام، فهو أساس بنيان كل مجتمع سليم، يعد من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي وهي سابقة على وجود الدولة ذاتها، لذلك حظيت الحياة الخاصة للأفراد بحماية دستورية وقانونية كبيرة من كافة الدول، وعلى رأسها المادة (12) من الإعلان العالمي لحقوق الإنسان الصادر في:1948/12/10[1] التي تنص على:" لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات". كما نصت على الخصوصية المادة (17) من العهد الدولي للحقوق المدنية والسياسية الصادر عن الهيئة نفسها بتاريخ:1966/12/16 [2]على:" لا يجوز التدخل بشكل تعسفي أو غير قانوني بخصوصيات أحد أو بعائلته أو ببيته أو مراسلاته .كما لا يجوز التعرض بشكل غير قانوني لشرفه أو سمعته .ولكل شخص الحق في حماية القانون ضد التدخل أو التعرض".

سنتطرق إلى مفهوم حرمة الحياة الخاصة في (الفرع الأول)، ثم نتناول صور الاعتداء عليها باستعمال الوسائل التقنية في (الفرع الثاني).

الفرع الأول: مفهوم حرمة الحياة الخاصة:

تعتبر الخصوصية من المواضيع المتجددة باستمرار، فإذا كانت الوسائل التقليدية المستعملة في المساس بخصوصية الأفراد كالقذف والسب والإهانة لا تشكل صعوبة ويمكن مجابهتها بالنصوص التقليدية لقانون العقوبات، فإن الأمر يختلف الآن بسبب تأثر الخصوصية بالتطورات المستمرة في مجال تكنولوجيات الإعلام والاتصال، إذ تمكّن تقنية المعلومات الجديدة الدوائر والوكالات الحكومية من خزن واسترجاع وتحليل كميات هائلة من البيانات الشخصية بما يتيح تتبع الفرد في الزمان وفي المكان المناسبين[3]. وهي جميعها تمثل تهديدا جدّيا على الحياة الخاصة وللحريات الفردية خاصة

---

[1] انضمت الجزائر إلى الإعلان العالمي لحقوق الإنسان غداة الاستقلال بموجب نص المادة (11) من دستور 1963 الصادر بتاريخ:1963/09/08التي تنص على: "توافق الجمهورية على الإعلان العالمي لحقوق الانسان ، وتنضم إلى كل منظمة دولية تستجيب لمطامح الشعب الجزائري، وذلك اقتناعا منها بضرورة التعاون الدولي".

[2] انضمت الجزائر إلى العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، والعهد الدولي الخاص بالحقوق المدنية والسياسية والبروتوكول الاختياري المتعلق بالعهد الدولي الخاص بالحقوق المدنية والسياسية الموافق عليها من طرف الجمعية العامة للأمم المتحدة بتاريخ:1966/12/16، بموجب المرسوم الرئاسي رقم :67/89 المؤرخ في:1989/05/16، (ج.ر) رقم:20 المؤرخة في:1989/05/17، ص ص531-532.

[3] *Myriam Quéméner et Yves Charpenel,Op.Cit,p.96.*

بصورتها المستحدثة والمتمثلة في بنوك المعلومات[1]، بحيث تتزايد معه مخاطر التقنيات الحديثة على حماية الخصوصية، كتقنيات رقابة (كاميرات) الفيديو، وبطاقات الهوية الإلكترونية، وقواعد البيانات الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات، ورقابة بيئة العمل وغيرها...إلخ . حيث تمثل مجالا خصبا لارتكاب كافة أشكال الجرائم الإلكترونية مثل ما وقع بمدينة عنابة في سنة 2013 أين قامت مجموعة من الأشخاص بإنشاء صفحة للشذوذ الجنسي على موقع التواصل الاجتماعي فيسبوك *(facebook)* وانتهكوا حرمة أساتذة وأبناء شخصيات وصناعيين معروفين. كل هذا يخلق صعوبات بالغة سواء على مستوى التجريم والعقاب أو على مستوى الإجراءات المتخذة لضمان عدم اللاّعقاب.

بالرجوع إلى مفهوم حرمة الحياة الخاصة أو الحق في الخصوصية، من الصعب وضع تعريف لها، لأن تعريف هذا الحق يرتبط بالتقاليد والثقافة والقيم الدينية السائدة والنظام السياسي في كل مجتمع. فضلاً عن ذلك فإن أغلب التشريعات اتجهت إلى عدم إيراد تعريف للحق في الخصوصية وتركت ذلك للفقه والقضاء، واكتفت بوضع نصوص تكفل حماية الحق وتعدد صور الاعتداء عليه. ويرجع السبب في ذلك إلى كون فكرة الحياة الخاصة فكرة مرنة ليس لها حدود ثابتة، فهي لا تختلف باختلاف الأقطار والأزمان فحسب، بل باختلاف الأشخاص أنفسهم بحسب أعمارهم وشخصياتهم وما يستدلون به من حرمة على خصوصياتهم[2] .

في الشأن نفسه، يعرف جانب من الفقه الحياة الخاصة على أنها: "الحق في أن يترك الإنسان وحيدا"[3] أو: "أن يعيش الشخص كما يحلو له وأن يعيش مستمتعا بممارسة أنشطة خاصة معينة حتى لو كان سلوكه على مرأى من الناس"[4]، كما يرى جانب آخر من الفقه أن الحق في الحياة الخاصة والحقوق الشخصية يكادان يكونان متطابقين لأنهما يقرّران حق الفرد في حماية اسمه ومراسلاته واتصالاته وشرفه واعتباره وحياته المهنية والعائلية وكل ما له تأثير على حياته الشخصية"[5]. من جهة أخرى يقصد بمفهوم حرمة الحياة الخاصة ضمن مجال المعلوماتية: "تلك البيانات التي تحتويها أجهزة الحواسيب عبر بنوك المعلومات"[6].

---

1 حسين الغافري، ومحمد الألفي، المرجع السابق، ص70.

2 حسين بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص110، راجع أيضا، الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، بحث فقهي مقارن، دار الفكر الجامعي، الإسكندرية، مصر، ط1، 2011، ص81 وما بعدها.

3 حنان ريحان مبارك المضحكي، المرجع السابق، ص324.

4 التعريف للفقيهين:*(Warren)* و*(Brandeis)*، حنان ريحان مبارك المضحكي، المرجع السابق، ص324.

5 نهلا عبد القادر المومني، المرجع السابق، ص166.

6 صبرينة بن سعيد، حماية الحق في حرمة الحياة الخاصة في عهد تكنولوجيا الإعلام والاتصال، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2015، ص124.

بدوره لم يعرف المشرع الجزائري حرمة الحياة الخاصة للأشخاص واعتبرها من الحقوق الشخصية للإنسان، هذه الحقوق ترتبط بكيان الشخص كي يعيش في طمأنينة، ولهذا نص في المادة (46) من التعديل الدستوري لسنة 2016 على أنه " لا يجوز انتهاك حرمة حياة المواطن الخاصة و رمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة..."، في الصدد نفسه، نصت المادة (4) من الدستور على" تضمن الدولة عدم انتهاك حرمة المسكن...". كما وفرت المادة (47) من القانون (ق.م.ج) حماية غير مباشرة للحقوق اللّصيقة بالشخصية، حينما نصت على:" لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء والتعويض عما يكون قد لحقه من ضرر". كما نص المشرع على بعض هذه الحقوق بموجب نصوص خاصة مثل: الحق في عدم انتهاك سرية المراسلات بموجب المادة (105) من القانون رقم:2000-03المؤرخ في:2000/08/05[1] يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، بل والعقوبة على ذلك في حالة فض أو اختلاس أو إتلاف رسائل مسلمة للبريد، حيث أحالت المادة (127) منه إلى تطبيق نص المادة (137) (ق.ع.ج). كما نص أيضا على سرية البيانات المتعلقة بالتصديق الإلكتروني بنص المادتان(42 -43) من القانون رقم:15-04 المؤرخ في:2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، إذ تنص المادة (42) منه على:" يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سريّة البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة...".

من جهة أخرى نص المشرع الجزائري على الحماية الجزائية لبعض الحقوق اللصيقة بالشخصية مثل:

- الحق في حرمة المنزل(المادة 295 ق.ع.ج).
- تجريم الأفعال الواقعة على شرف واعتبار الأشخاص (296 - 299 ق.ع.ج) .
- إفشاء السر المهني (المادة 301 ق.ع.ج).
- الحق المراسلات (المادة303 ق.ع.ج).

تعتبر هذه الحماية الجزائية حماية غير مباشرة، ومع تطور مجالات استعمال تكنولوجيات الإعلام والاتصال وإساءة استخدامها، أصبحت غير كافية ولا يمكن ضمان الحقوق الخاصة للأفراد في ظل هذا المناخ، سوى بتدخل جديد من المشرع الجزائري لمواجهة هذا النوع المستحدث من

[1] تنص المادة (4/105) من القانون رقم:2000-03 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السّلكية واللاّسلكية على: "لا يمكن بأي حال من الأحوال انتهاك سرية المراسلات".

الجرائم، فكان ذلك بالقانون رقم:06-23 المؤرخ في:2006/12/23 المعدل والمتمم لقانون العقوبات بموجب المواد من:(303 مكرر - 303 مكرر3)، و هذا ما سنتناوله في الفرع الوالي.

الفرع الثاني: صور الاعتداء على حرمة الحياة الخاصة:

نص المشرع الجزائري على حرمة الحياة الخاصة للأفراد بموجب نصوص المواد من:(303 مكرر - 303 مكرر3) (ق.ع.ج) منسجما في ذلك مع نصوص (إ.أ.م.إ.م)، و أيضا نص المادة (14) من (إ.ع.م.ج.ت.م) التي تنص على تجريم:" الاعتداء على حرمة الحياة الخاصة بواسطة تقنيات المعلومات". كما تقابل المادة (303 مكرر) (ق.ع.ج) نص المادة (1/226) (ق.ع.ف)[1] التي جرّمت أفعال المساس بحرمة الحياة الخاصة.

أولا: جريمة التقاط الأحاديث والصور دون رخصة:

أ-**الركن الشرعي:** نصت المادة(303 مكرر) من(ق.ع.ج) على:" يعاقب بالحبس من (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.

2-التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه...".

ب- **الركن المادي:** يتمثل في العناصر الآتية:

- تعلق الأفعال بالحياة الخاصة للفرد.
- التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية.
- التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص.
- استخدام الوسائل التقنية مهما كان نوعها.
- حدوث الفعل بغير رضا المجنى عليه.

---

[1] ***Article 226-1 De l'atteinte à la vie privée. du (CPF) :***

"Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles Prononcées à titre privé ou confidentiel.

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé…"

عرفته المادة (8/02) من (إ.ع.م.ج.ت.م) على أنه:" مشاهدة البيانات أو المعلومات أو الحصول عليها". وبهذا المعنى ينصرف فعل الالتقاط إلى الحصول على ما جرى بين الأشخاص من كلام أو ما تفوه به الفرد سرا ودون علمه، أما التسجيل يعني حفظ الحديث على جهاز أو أي وسيلة أخرى معدة لذلك، بقصد الاستماع إليه فيما بعد، أما النقل فيقصد به نقل الحديث أو المكالمة الذين تم الاستماع إليهما أو تسجيلهما من المكان الذي تم فيه إلى مكان آخر غيره، وذلك بأي وسيلة تقنية كما تتم هذه الأفعال دون رضا المجنى عليه حال وجوده في مكان خاص[1].

أما بخصوص الوسائل المستعملة، أورد المشرع الجزائري عبارة " بأي تقنية كانت" وهدفه من وراء ذلك استيعاب التطورات التقنية والتكنولوجية خاصة الدقيقة منها، كالأجهزة التي تستعمل تقنية الجزيئات متناهية الصغر *(nanotechnology)*، ويدخل في هذا المجال كافة الأجهزة الإلكترونية مثل: أجهزة مراقبة الصوت والصورة مثل: "كاميرات الفيديو" والهاتف النقال، كما تستعمل تقنية *(Bluetooth)*[2] أو تقنية *(SHAREit)*...إلخ، لنقل هذه الملفات بصورة سريعة جدا. حيث توضع هذه الأجهزة خلسة في الأماكن الخاصة دون علم الضحية بغية انتهاك حرمة حياته الخاصة.

من جهة أخرى يعتبر المكان الذي تقع فيه هذه الأفعال مكانا خاصا، على أساس أن المكان هو مستودع الخصوصية كالسكن والمكتب وغرف الفنادق...إلخ، و يقصد بالمكان الخاص المكان المغلق الذي لا يمكن أن تنفذ إليه نظرات الناس من الخارج إلا بموافقة مالكه. وتنسحب حماية القانون على كل من يوجد في هذا المكان أيا كانت صفته، أي سواء كان مالكا أو مستأجرا أو زائرا أو موجودا فيه بصفة عارضة لأي سبب كان[3].

نستنتج من الشروط السالفة الذكر أن المشرع الجزائري أخذ بالمعيار الموضوعي عندما نص على التقاط الأحاديث، فلا يهم هنا مكان تبادل أطراف الحديث بقدر ما يهم هل كان الحديث خاصا

---

[1] فضيلة عاقلي، الحماية القانونية للحق في حرمة الحياة الخاصة-دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة الإخوة منتوري قسنطينة، الجزائر، 2012، ص251.

[2] البلوتوث أو القارن *(Bluetooth)* :"هي تقنية اتصالات راديوية في نطاق الموجات القصيرة صممت لنقل البيانات لمسافات قصيرة من المتر الواحد إلى المائة متر وباستهلاك كميات ضئيلة من الطاقة، وتستخدم هذه التقنية بشكل كبير في نقل البيانات بين الأجهزة المحمولة وفى الملحقات الطرفية للحاسوب."، وعليه يستطيع مالكوا الهواتف النقالة خاصة الذكية منها تبادل كم كبير من البيانات سواء كانت ملفات صوتية أو فيديو، أو صور ونشرها على أوسع نطاق، للاطلاع أكثر على الموضوع يرجى زيارة الرابط الآتي: *https://ar.wikipedia.org/wiki/%D8%A8%D9%84%D9%88%D8%AA%D9%88%D8%AB*،تاريخ الاطلاع:2015/12/05 على الساعة:12:14.

[3] فضيلة عاقلي، الأطروحة السابقة، ص240.

أم لا؟، أما فيما يخص التقاط الصّور فإنه أخذ بالمعيار المكاني الذي يحظر التقاط الصور في الأماكن الخاصة ، بغير إذن أصاحبها أو رضاهم [1].

ج-الركن المعنوي: جريمة التقاط الأحاديث والصور بدون رخصة، جريمة عمدية بدليل قول المشرع:"...كل من تعمد المساس بحرمة الحياة الخاصة..."، إذ تتطلب القصد الجنائي العام الذي يقوم على علم الجاني بأن هذه الأفعال تشكل جريمة، إضافة إلى اتجاه إرادته للقيام بالسلوك المجرّم.

د-العقوبات المقررة: الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000دج إلى 300.00دج.

هـ-العقوبة على الشروع: معاقب عليه بنص المادة(303مكرر الفقرة3):"... يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة ويضع صفح الضحية حدا للمتابعة الجزائية".

و-العقوبات التكميلية: نصت عليها المادة(303 مكرر2):" يجوز للمحكمة أن تحظر على المحكوم عليه من أجل الجرائم المنصوص عليها في المادتين(303مكرر- 303 مكرر1) ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة (09 مكرر1)[2] لمدة لا تتجاوز خمس (5) سنوات. كما يجوز لها أن تأمر بنشر حكم الإدانة طبقا للكيفيات المبينة بالمادة (18) من هذا القانون. ويتعين دائما الحكم بمصادرة الأشياء التي استعملت لارتكاب الجريمة.

ثانيا: جريمة إعلان التسجيل أو الصور أو الوثائق:

أ- الركن الشرعي: تنص المادة (303 مكرر1) (ق.ع.ج)على:" يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير أو استخدم بأي وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة (303مكرر) من هذا القانون.عندما ترتكب الجنحة المنصوص عليها في الفقرة السابقة عن طريق الصحافة تطبق الأحكام الخاصة المنصوص عليها في القوانين ذات العلاقة لتحديد الأشخاص المسؤولين..."

---

1 صبرينة بن سعيد، الأطروحة السابقة، ص198.

2 تنص المادة (09 مكرر) من (ق.ع.ج) على:" العزل أو الإقصاء من جميع الوظائف والمناصب العمومية التي لها علاقة بالجريمة- الحرمان من حق الانتخاب أو الترشح ومن حمل أي وسام- عدم الأهلية لأن يكون مساعدا محلفا، أو خبيرا أو شاهدا على أي عقد، أو شاهدا أمام القضاء إلا على سبيل الاستدلال- الحرمان من الحق في حمل الأسلحة، وفي التدريس، وفي إدارة مدرسة أو الخدمة في مؤسسة للتعليم بوصفه أستاذا أو مدرسا أو مراقبا- عدم الأهلية لأن يكون وصيا أو قيما- سقوط حقوق الولاية كلها أو بعضها.

ب- **الركن المادي:** يقوم على العناصر الآتية:

- **فعل الاحتفاظ:** يعني إبقاء الشخص في حوزته التسجيل أو مستندا للغير عمدا مع علمه بمضمونه، متى كان هذا التسجيل أو المستند قد تم الحصول عليه بإحدى الطرق المبينة في المادة (303مكرر 1)[1]، كما يأخذ فعل الاحتفاظ شكلين أحدهما الاحتفاظ للغرض الشخصي، بمعنى احتفاظ الشخص بالتسجيلات والصور والوثائق للتمتع بها لوحده وإشباع تطفله، والثاني الاحتفاظ بها لفائدة الغير، حيث يتلقى الوثيقة شخص آخر سواء بصفته أمينا أو بصفته مودعا لديه بمقابل[2].

ما يلاحظ على المشرع الجزائري استعماله مصطلح "الاحتفاظ" في هذه الجنحة، هو نفسه يشكل جنحة إخفاء أشياء متحصلة من جريمة المنصوص عليها في المادة (387) (ق.ع.ج) التي تنص على:" ...كل من أخفى عمدا أشياء مختلسة أو مبددة أو متحصلة من جناية أو جنحة...".

- **فعل الإفشاء:** يتمثل في إعلام الجمهور وهي الصورة الأكثر خطورة للإفشاء للغير بمحتوى التسجيلات والصور والوثائق باستعمال كافة وسائل الاتصال التي توفرها التقنية الحديثة وخاصة شبكة الإنترنت[3].

- **فعل الاستعمال:** و يعني استخدام التسجيل أو المستند أو الوثائق لتحقيق غرض ما يتمثل في المساس بحرمة الحياة الخاصة للأفراد، وسواء كان علنا أم غير ذلك، وما يلاحظ أن المشرع الجزائري لم يشترط حصول العلانية شأنه في ذلك شأن المشرع الفرنسي[4].

ج-الركن المعنوي: جريمة إعلان التسجيل أو الصور أو الوثائق جريمة عمدية يتطلب ركنها المعنوي القصد الجنائي العام، الذي يقوم على عنصري العلم والإرادة، فيجب أن يكون الجاني عالما بمصدر الحصول على التسجيل أو الصور أو المستند، وأن إعلانه لها يشكل جريمة. كما يجب أن تتجه إرادة الجاني إلى إذاعة التسجيل أو المستند أو تسهيل إذاعته أو استعماله، أما إذا تم ذلك على سبيل الخطأ، فلا تقوم الجريمة لانتفاء الركن المعنوي.

د-العقوبات المقررة: الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000دج إلى 300.00دج.

---

1 فضيلة عاقلي، الأطروحة السابقة، ص269.

2 عبد العزيز نويري، الحماية الجزائية للحياة الخاصة-دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر،2011، ص152.

3 الأطروحة نفسها، ص145.

4 فضيلة عاقلي، الأطروحة السابقة، ص269.

هـ-العقوبة على الشروع: معاقب عليه بنص المادة (303مكرر3/1):"... يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة. ويضع صفح الضحية حدا للمتابعة الجزائية".

و-العقوبات التكميلية: نصت عليها المادة(303مكرر2):" يجوز للمحكمة أن تحظر على المحكوم عليه من أجل الجرائم المنصوص عليها في المادتين (303مكرر - 303 مكرر1) ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة (09مكرر1) سابقة الذكر لمدة لا تتجاوز خمس (5) سنوات. كما يجوز لها أن تأمر بنشر حكم الإدانة طبقا للكيفيات المبينة بالمادة (18) من هذا القانون. ويتعين دائما الحكم بمصادرة الأشياء التي استعملت لارتكاب الجريمة".

ز- عقوبة الشخص المعنوي: نصت المادة (303مكرر3) على تحميل الشخص المعنوي المسؤولية الجزائية في حال ارتكابه هذه الأفعال، حيث تنص على:" يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم المحددة في الأقسام 3 و4 و5 من هذا الفصل، وذلك طبقا للشروط المنصوص عليها في المادة51 مكرر. وتطبق على الشخص المعنوي عقوبة الغرامة حسب الكيفيات المنصوص عليها في المادة 18 مكرر، وفي المادة 18مكرر 2 عند الاقتضاء. ويتعرض أيضا لواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 18 مكرر".

ثالثا: ارتكاب هذه الجرائم من طرف الصحافة: نظرا للدور البارز الذي يلعبه الإعلام بكافة أشكاله في عصرنا الحالي، سواء المرئي منه أو المسموع أو المقروء أو الإلكتروني، ومع انتشار الجرائد الإلكترونية والقنوات الفضائية الجزائرية الخاصة، وبهدف الحد من إساءة استخدام هذا الفضاء نص في المادة (303مكرر2/1) على ارتكاب هذه الأفعال المبينة في نص المادة سالفة الذكر من طرف الصحافة حيث تنص على:"... عندما ترتكب الجنحة المنصوص عليها في الفقرة السابقة عن طريق الصحافة تطبق الأحكام الخاصة المنصوص عليها في القوانين ذات العلاقة، لتحديد الأشخاص المسؤولين..."و بالتالي أحالنا المشرع الجزائري إلى تطبيق جملة القوانين المتعلقة بجنح الصحافة.

بناء على ما سبق ذكره، نص المشرع الجزائري ضمن قانون العقوبات على الجرائم المتعلقة بالإهانة أو السب أو القذف باستعمال الوسائل الإلكترونية، إضافة إلى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وأيضا الجرائم الماسة بحرمة الحياة الخاصة باستعمال الوسائل التقنية وهو مسلك حسن في سياسته الجنائية الرامية إلى مكافحة هذا النوع المستحدث من الجرائم. لكن بالمقابل لم يكتف المشرع بفعل ذلك ضمن إطار القانون العام، بل تعدى ذلك إلى نطاق القانون الخاص، وهذا ما سنراه في المبحث الموالي.

المبحث الثاني: مكافحة الجرائم الإلكترونية بموجب نصوص خاصة

لم يتوقف المشرع الجزائري في سياسته الجنائية الرامية إلى مكافحة كافة أشكال الإجرام الإلكتروني بتعديل قانون العقوبات بموجب القانون رقم:04-15 المتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات وقانون الإجراءات الجزائية بموجب القانون رقم:09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بل تعدى ذلك إلى مجالات يحكمها القانون الخاص وتستخدم في نشاطها الوسائل الإلكترونية، وهذا رغبة منه في توسيع دائرة التجريم والعقاب لردع هذا النوع المستحدث من الجرائم، خاصة في ظل توجه الدولة الجزائرية نحو الحكومة الإلكترونية وما يفرضه ذلك من تحديات متعلقة بأمن المعلومات من حيث السرية والسلامة والتكامل والوفرة.

سنتطرق في هذا المبحث إلى مكافحة الجرائم الإلكترونية بموجب القانون رقم:2000- 03 المؤرخ في:2000/08/05 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية في (المطلب الأول)، ثم نتناول مفهوم التجارة الإلكترونية ونظام الدفع الإلكتروني إضافة إلى التعرف على واقع التجارة الإلكترونية في الجزائر وبعض وسائل الدفع الإلكتروني والحماية المقررة لها، في(المطلب الثاني)، ثم نتطرق إلى جرائم التقليد المتعلقة بحماية برامج الحاسوب وقواعد البيانات في (المطلب الثالث)، لنختم في الأخير بالحديث عن جرائم التوقيع والتصديق الإلكترونيين في (المطلب الرابع).

المطلب الأول: مكافحة الجرائم الإلكترونية بموجب قانون البريد والمواصلات السّلكية واللاّسلكية

يعتبر قطاع المواصلات السلكية واللاسلكية أحد القطاعات الحساسة في الدولة، فهو يتعلق بنقل المعلومات إلكترونيا سواء الخاصة بالدولة ومؤسساتها أو بالأشخاص الطبيعية. فكان على المشرع أن يمدد من سياسته الجنائية في مجال مكافحة الجرائم الإلكترونية إلى هذا القطاع الحساس بما يخدم أمن المعلومات المرسلة وسريتها، وبما يضمن أيضا أمن الدولة ومؤسساتها وحرمة الحياة الخاصة للأفراد، سنتناول بصفة موجزة هذه الجرائم على أساس اعتمادنا على المفهوم الموسع للجريمة الإلكترونية والتي تتم بأية وسيلة إلكترونية. وعليه سنبدأ بالجرائم الماسة بسرية ومضمون المراسلات بواسطة اللاّسلكي في (الفرع الأول)، ثم نتطرق إلى الجرائم الواقعة باستعمال إشارات ورسالات اللاّسلكي في (الفرع الثاني).

الفرع الأول: الجرائم الماسة بسرية ومضمون المراسلات بواسطة اللاسلكي:

سندرس هذه الجرائم في إطار القانون رقم:2000-03 المتعلق بالبريد والمواصلات السلكية واللاّسلكية، حيث عرفت المادة (9/08):"يقصد في مفهوم هذا القانون...شبكة المواصلات السلكية[1] واللاّسلكية: كل منشأة أو مجموعة منشآت تضمن إما التراسل وإما تراسل وإرسال إشارات المواصلات السلكية واللاسلكية وكذا تبادل معلومات التحكم والتسيير المشتركة ما بين النقط الطرفية لهذه الشبكة" كما نصت المادة (10/08-11) على أنواع الشبكات فقد تكون شبكة داخلية[2]. أو شبكة خاصة[3] من جانب آخر أورد المشرع الجزائري تعريفا للاتصالات الإلكترونية بموجب نص المادة (02/و) من القانون رقم:09-04 السابق ذكره على أنها:" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية." وعليه لم يحدد المشرع الوسيلة الإلكترونية المستعملة مما يترك الباب مفتوحا أمام أي وسيلة تظهر في المستقبل تبعا لتطور تكنولوجيات الإعلام والاتصال.

أولا: جريمة انتهاك سرية المراسلات بواسطة المواصلات السلكية واللاّسلكية:

أ- **الركن الشرعي:** نصت المادة (2/127) من القانون رقم:2000-03 على: "تطبق العقوبات المنصوص عليها في المادة (137) من(ق.ع.ج)...تسري نفس العقوبات على كل شخص مرخص له بتقديم خدمات مواصلات سلكية ولاسلكية وكل عامل لدى متعاملي الشبكات العمومية للمواصلات السلكية واللاّسلكية والذي في إطار ممارسة مهامه وزيادة على الحالات المقررة قانونا، ينتهك بأي طريقة كانت سرية المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق المواصلات السلكية اللاسلكية أو الذي أمر أو ساعد في ارتكاب هذه الأفعال..."

ب- **الركن المادي:** يشتمل الركن المادي في هذه الجريمة على:

- انتهاك سرية المراسلات الصادرة.
- انتهاك سرية المراسلات المرسلة.

---

[1] عرّف الاتحاد الدولي للاتصالات: الاتصالات اللاّسلكية هي: مصطلح عام لخدمات الاتصالات المتنقلة التي لا تستخدم شبكات للخطوط الثابتة للنفاذ مباشرة إلى المشترك"، كما تعرف ايضا على أنها:" الاتصال من الجهاز اللاّسلكي(يدعم التقنية اللاّسلكية) من أي منطقة دون أية أسلاك تربطه"، فيتم الاستغناء عن الأسلاك وتوفير خدمات الاتصالات المختلفة للمستخدمين في كل مكان: في المنزل في السيارة، في الطائرة...إلخ، لأكثر تفاصيل يرجى الاطلاع على موقع الاتحاد الدولي للاتصالات: *http://www.itu.int/ar/pages/default.aspx* ، تاريخ الاطلاع:2015/12/15 على الساعة:16:48 .

[2] تنص المادة (10/08) من القانون رقم:2000- 03 على: "شبكة داخلية: شبكة مستقلة تنشأ كلها على نفس الملكية دون استعمال الأملاك العمومية بما فيها الأملاك الهيرتيزية أو أية ملكية أخرى .

[3] تنص المادة (11/08) من القانون رقم:2000- 03 على:" شبكة خاصة: شبكة مواصلات سلكية ولاسلكية مخصصة إما للاستعمال الخاص...وإما للاستعمال المشترك...".

- انتهاك سرية المراسلات المستقبلة.

- الوسائل المستعملة: يمثل انتهاك سرية المراسلات الاعتداء على حق دستوري مكفول وهو يمثل الاعتداء على حرمة الحياة الخاصة للأفراد بأي طريقة كانت وباستعمال وسائل المواصلات السلكية واللاّسلكية مثل: الفاكس، التيلكس...إلخ.

- **صفة الجاني:** وهما: مقدمو خدمات المواصلات السلكية واللاسلكية، وكل عامل لدى متعاملي الشبكات العمومية للمواصلات السلكية واللاسلكية، إضافة إلى حالات أخرى يقرّرها القانون.

ج-الركن المعنوي: جريمة انتهاك سرية المراسلات بواسطة المواصلات السلكية واللاسلكية جريمة عمدية تتطلب القصد الجنائي العام الذي يقوم على علم الجاني بأنه ينتهك سرية المراسلات وأن هذا الفعل معاقب عليه قانونا، إضافة إلى اتجاه إرادته إلى القيام بهذه الأفعال.

د-العقوبات المقررة: تنص المادة (137) (ق.ع.ج) على:" كل موظف أو عون...يعاقب بالحبس من (3) أشهر إلى خمس (5) سنوات وبغرامة من 30.000 دج إلى 500.000 دج . ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق يختلس أو يتلف برقية أو يذيع محتواها".

كما نصت المادة (3/127) على معاقبة كل شخص خارج الأشخاص المذكورين في الفقرتين السابقتين يقوم بالأفعال السابق ذكرها، فنصت على: "يعاقب بالحبس من شهرين(2) إلى سنة وبغرامة مالية من 50.000دج إلى 1.000.000دج أو بإحدى هاتين العقوبتين كل شخص غير الأشخاص المذكورين في الفقرتين السابقتين ارتكب أحد الأفعال المعاقب عليها بموجب هاتين الفقرتين".

هـ-العقوبات التكميلية: المنع من ممارسة كل نشاط أو مهنة في قطاع المواصلات السلكية واللاسلكية أو قطاع البريد أو في قطاع ذي صلة بهذين القطاعين لمدة تتراوح بين (1) سنة إلى (5) سنوات، وهذا حسب نص المادة (3/127)

ثانيا: جريمة إفشاء مضمون المراسلات بواسطة اللاسلكي:

أ- الركن الشرعي: تنص المادة (137) من القانون رقم:2000-03 على: "يعاقب بالعقوبات المنصوص عليها في المادة 137 من قانون العقوبات، كل شخص يفشي أو ينشر أو يستعمل دون ترخيص من المرسل أو المرسل إليه، مضمون المراسلات المرسلة عن طريق اللاسلكي الكهربائي أو يخبر بوجودها".

ب- الركن المادي: يتمثل في:

- أفعال الإفشاء أو النشر أو الاستعمال -تم شرحها سابقا بخصوص التلاعب في المعطيات خارج المنظومة المعلوماتية- لمضمون المراسلة أو إعلام الغير بوجودها، وذلك باستعمال الأجهزة الإلكترونية مثل: أجهزة الاتصال اللاّسلكي.

- عدم موافقة المرسل أو المرسل اليه.

كما لا يشترط قيام الجاني بكافة الأفعال المذكورة، بل يكفي قيامه بفعل واحد لتتحقق الجريمة.

ج-الركن المعنوي: جريمة إفشاء مضمون المراسلات بواسطة الأجهزة اللاسلكية، جريمة عمدية تتطلب القصد الجنائي العام الذي يقوم على علم الجاني بأنه يقوم بأفعال الإفشاء أو النشر أو الاستعمال أو الإخبار لمضمون المراسلات، وأن هذا الفعل معاقب عليه قانونا، إضافة إلى اتجاه إرادته إلى القيام بهذه الأفعال.

د-العقوبات المقررة: الحبس من (3) أشهر إلى خمس (5) سنوات وبغرامة من 30.000 دج إلى 500.000 دج، حسب نص المادة (137) (ق.ع.ج).

الفرع الثاني: الجرائم الواقعة باستعمال إشارات وإرسالات اللاّسلكي: سنتطرق إليها كما يأتي:

أولا: جريمة إصدار إشارات أو نداءات عن طريق اللاّسلكي:

أ- الركن الشرعي: تنص المادة (135) من القانون رقم: 2000-03 على:" يعاقب بالحبس من شهرين(2) إلى سنة وبغرامة مالية من 10.000دج إلى 100.00دج أو بإحدى هاتين العقوبتين كل شخص يصدر عمدا عن طريق لاسلكي كهربائي إشارات أو نداءات نجدة كاذبة أو خادعة".

ب- الركن المادي: يتمثل الركن المادي في قيام الجاني بإصدار إشارات أو توجيه نداء كاذب أو خادع، باستعمال أجهزة اللاّسلكي. كما لا يشترط قيام الجاني بكافة الأفعال المذكورة، بل يكفي قيامه بفعل واحد لتتحقق الجريمة.

ج-الركن المعنوي: استعمل المشرع مصطلح "عمدا"، يتطلب فيها القصد الجنائي العام الذي يقوم على علم الجاني بأن هذا الفعل يشكل جريمة معاقبا عليها قانونا، إضافة إلى اتجاه إرادته إلى القيام بهذه الأفعال. فإذا ثبت ارتكاب الفعل عن طريق الخطأ ينتفي معه الركن المعنوي.

د-العقوبات المقررة: الحبس من شهرين(2) إلى (1) سنة وبغرامة مالية من 10.000دج إلى 100.00دج أو بإحدى هاتين العقوبتين.

د-العقوبة التكميلية: مع مراعاة الغير حسن النية، يحكم القاضي بمصادرة الأجهزة حسب نص المادة (137).

ثانيا: جريمة الإرسال اللاسلكي باستعمال رمز نداء:

أ- الركن الشرعي: تنص المادة (136) من القانون رقم:2000-03 على: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة كل شخص يقوم بإرسالات لاسلكية كهربائية باستعمال، عمدا رمز نداء في السلسلة الدولية مخصص لإحدى محطات الدولة أو لكل محطة أخرى مرخص بها".

ب- الركن المادي: يتمثل في فعل الإرسال العمدي بواسطة المواصلات اللاسلكية وباستعمال رمز نداء خاص بمحطات الدولة أو أي محطة أخرى مرخصة.

ج-الركن المعنوي: هي جريمة عمدية بدليل استعمال المشرع كلمة "عمدا"، يتطلب فيها القصد الجنائي العام الذي يقوم على علم الجاني بأن هذا الفعل يشكل جريمة معاقب عليه قانونا، إضافة إلى اتجاه إرادته إلى إتيان النشاط المجرّم.

د-العقوبات المقررة: الحبس من ثلاثة (3) أشهر إلى سنة.

ما يلاحظ على المشرع الجزائري في سياسته التجريمية والعقابية بخصوص الجرائم الإلكترونية المرتكبة في هذا القطاع الحسّاس هو عدم اتسامها بالتشدد، رغم ما تشكله هذه الجرائم من خطورة سواء على أمن الدولة أو حرمة الحياة الخاصة للأفراد في ظل التطور التكنولوجي الذي تعرفة وسائل المواصلات السلكية واللاسلكية.

المطلب الثاني: التجارة الإلكترونية

أدت التكنولوجيا الحديثة في مجال تقنية المعلومات خاصة ما تعلق بانتشار شبكة الإنترنت وكثرة استعمالاتها إلى بروز نوع جديد من التجارة يسمى بالتجارة الإلكترونية، فرغم ميزاتها الظاهرة إلا أنها تنطوي على مخاطر عديدة، بحيث تعتمد التجارة الإلكترونية على نظام الدفع الإلكتروني الذي يقوم على أدوات ووسائل إلكترونية قصد تسهيل التعاملات المالية(الفرع الأول)، مما دفع بالمشرع الجزائري إلى توفير الحماية الجزائية والفنية لنظام الدفع الإلكتروني بهدف عدم إساءة استخدامه في (الفرع الثاني).

الفرع الأول: مفهوم التجارة الإلكترونية ونظام الدفع الإلكتروني:

لقد شهد العالم في الآونة الأخيرة اهتماما متزايدا بالتجارة الإلكترونية (*E- Commerce*) كنتيجة حتمية وضرورية للتطورات والمستجدات الحديثة في مجال تكنولوجيا المعلومات والاتصالات إلا أنها لا تخلو من مخاطر عديدة لاعتمادها تقنية المعلومات. كما أننا سنتعرف على واقع التجارة

الإلكترونية وبعض وسائل الدفع الإلكتروني المعتمدة في الجزائر قصد إلقاء الضوء على السياسة الجنائية للمشروع الجزائري بخصوص الجرائم الإلكترونية الواقعة في هذا المجال.

أولا: مفهوم التجارة الإلكترونية، مخاطرها وواقعها في الجزائر:

أ- **تعريف التجارة الإلكترونية:** ظهرت التجارة الإلكترونية منذ ثلاثة عقود مضت ثم تطور مفهومها خلال الربع الأخير من القرن الماضي بتطور الأجهزة الإلكترونية، هدفها تقديم خدمات مالية وسريعة للعميل. ومع انتشار شبكة الإنترنت تحوّل العديد من شركات الأعمال إلى استخدامها والاستفادة من مزاياها، وانعكس ذلك على الحياة الاقتصادية للمستهلكين فأصبح بإمكان المستهلك التسوّق وإتمام كافة تعاملاته المالية والمصرفية وهو جالس في بيته[1]. هناك الكثير من التعريفات للتجارة الإلكترونية منها:" هي نظام إلكتروني يتيح التعامل في السلع والخدمات في صيغة افتراضية أو رقمية، وتنفيذ العقود المتعلقة بهذه السالع والخدمات[2]"، أو هي:" استخدام تكنولوجيا المعلومات لايجاد الروابط الفعالة بين الشركاء في التجارة"[3]، أو هي:" تلك العملية التجارية التي تتم بين طرفين-البائع والمشتري- وتتمثل في عقد الصفقات وتسويق المنتجات عن طريق استخدام الحاسب الإلكتروني عبر شبكة الإنترنت وذلك دون الحاجة لانتقال الطرفين أو لقائهما، بل يتم التوقيع إلكترونيا على العقد"[4].

إن التجارة الإلكترونية تمثل اليوم الأساس في عالم التجارة، ويؤكد العارفون بأنها ستكون الأساس الوحيد للتعامل في السنوات القادمة، كما ستعرف منافسة كبيرة سواء من طرف التلفزة التفاعلية أو جهاز الهاتف النقال الذكي، وبالتالي لن يخرج النشاط التجاري عن التعامل الإلكتروني الذي حقق في المدة الاخيرة أرقاما عالية تعد بالمليارات وتهافت التجار على ضمان مواقع لهم عبر شبكة الإنترنت بغية تحقيق الإنتشار التجاري السريع وغزو السوق الدولي، كما تتميز التجارة الإلكترونية في طبيعتها عن التجارة التقليدية بما يأتي[5]:

- إجراء المعاملات والعقود التجارية من خلال شبكة الإنترنت.

---

[1] *Alain Bensoussan, Internet, Op.Cit,p.117.*

[2] عصام عبد الفتاح مطر، المرجع السابق، ص18.

[3] جلول بن عناية وحواسني يمينة، مفاهيم أساسية حول الإنترنت والتجارة الإلكترونية، الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر - عرض تجارب دولية -المركز الجامعي خميس مليانة - الجزائر، يومي:26-27 أفريل 2011 ، ص14.

[4] عبد الفتاح بيومي حجازي، نحو صياغة، المرجع السابق، ص69.

[5] علي كحلون، الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الإلكترونية، دار اسهامات في أدبيات المؤسسة، تونس،2002 ص158.

- نقل المعلومات والعمليات التجارية على اختلاف أنواعها عبر الشبكة.
- استخدام ما تتيحه شبكة الإنترنت من إمكانات ضخمة سواء ما تعلق بالصوت أو الصورة أو الحركة.

ب- مخاطر التجارة الإلكترونية: تنبع مخاطر التجارة الإلكترونية وبشكل رئيس من مخاطر شبكة الإنترنت، فمخاطر كثيرة ومتعددة، وليس من السهل حصرها فتكنولوجيا التجارة الإلكترونية متطورة وسريعة وكل تطور تنتج عنه مخاطر جديدة، فبالإضافة إلى تعرض بطاقات الائتمان للسرقة والضياع الذي ينتج عنه الاستعمال الاحتيالي، يكمن الخطر الرئيس في التجارة الإلكترونية في إمكانية اختراق قراصنة المعلوماتية للأنظمة المعلوماتية للشركات ووسائل الدفع الإلكتروني، وذلك باستعمال البرمجيات الخبيثة، قصد الحصول على المعلومات الخاصة لكل من المستهلك والشركات حيث تتسبب عمليات الاختراق هذه في أضرار كبيرة على الشركات أكثر منه على المستهلك، إذ أن تعويض خسارة المشتري ممكنة، في حين تتكبد الشركة الخسائر بفقدانها الإيرادات والتي يصعب تعويضها أو حتى تعقب المتلاعبين بأنظمتهم المحاسبية، وذلك نظرا لتعقيدات العمليات الكثيرة في التجارة الإلكترونية، لذا لابد من تأمين هذه البيئة الإلكترونية التي يجري فيها النشاط التجاري بما يخدم الثقة والائتمان بين أطرافه(1).

على الرغم من الانتشار الواسع لشبكة الإنترنت وكثرة مستعمليها وبروز بعض التعاملات الإلكترونية وتوجه الجزائر نحو الحكومة الإلكترونية، لازال المشرع الجزائري متأخرا في وضع الإطار القانوني لممارسة التجارة الإلكترونية وحمايتها جنائيا رغم مخاطرها الكبيرة، وهذا على غرار المشرع الفرنسي والمشرع التونسي الذي قام بذلك بموجب القانون رقم:2000-83 المؤرخ في 09 أوت 2000المتعلق بالمبادلات والتجارة الإلكترونية، فمخاطر التجارة الإلكترونية تجعل الحاجة ملحّة لحماية المعاملات الإلكترونية المبنية على عنصري الثقة والائتمان من الجرائم التي تقع عليها خاصة بعد التوجه نحو الحكومة الإلكترونية، إضافة إلى الخسائر الفادحة التي قد تلحقها هذه الجرائم بالاقتصاد الوطني، ناهيك عن عدم كفاية التشريعات الجنائية القائمة لمواجهة الاعتداءات التي قد تنصب على المعاملات التجارية الإلكترونية(2).

ج- واقع التجارة الإلكترونية في الجزائر: رغم التطوّر السريع الذي شهدته الجزائر في استخدام التكنولوجيات الحديثة، إلاّ أن ذلك لم ينعكس على كلّ مناحي الحياة اليومية للجزائريين، ومنها

---

[1] لمزيد من التفاصيل حول عملية تأمين النشاط التجاري في البيئة الإلكترونية، راجع، عصام عبد الفتاح مطر، المرجع السابق، ص ص50-65، وأيضا، الشحات ابراهيم محمد منصور، المرجع السابق، ص114.

[2] لمزيد من التفاصيل حول مخاطر التجارة الالكترونية، راجع، سمية ديمش، التجارة الإلكترونية حقيقتها وواقعها في الجزائر، مذكرة ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، قسم العلوم الاقتصادية، جامعة منتوري، قسنطينة، الجزائر، 2011، ص ص61-63.

المعاملات التجارية التي مازالت تتم وفق الأنماط التجارية التقليدية، في ظل حضور محتشم للمعاملات الإلكترونية، حيث لم يبلغ عدد مواقع التجارة الإلكترونية في سنة 2009 إلا ستون(60) موقعا لشركات وخواص يبيعون منتجاتهم إلكترونيا، وهو رقم جد متواضع[1]. فبرغم المجهودات المبذولة من طرف الدولة في تطوير نظم الدفع الإلكتروني الذي يعتبر أحد مظاهر الحكومة الإلكترونية التي تطمح الجزائر إلى تحقيقها مثل: إصدار بطاقة الصرّاف الآلي*(ATM)*، وبطاقة ما بين البنوك *(CIB)*، لم تنطلق رسميا خدمة الدفع الإلكتروني إلا بتاريخ: 2016/10/03 يشترك فيها 11 بنكا و9 مؤسسات توفر هذه الخدمة لزبائنها، حيث ستسمح هذه الخدمة بتدعيم التجارة الإلكترونية وفتح الطريق أمام اقتصاد رقمي.[2] وهو ما سيفتح الباب واسعا أمام وقوع جرائم إلكترونية جديدة في هذا الفضاء الإلكتروني. ورغم هذا ما زال التسوّق الإلكتروني واقتناء السلع بضغطة زر بالنسبة لغالبية الجزائريين بعيد المنال قد يطول تحققه وهذا نتيجة لعقبات كثيرة نذكر منها:

- انعدام الثقة لدى الجزائريين في التعاملات غير النقدية، نتيجة التعاملات البدائية للبنوك والمؤسسات المالية الجزائرية، حيث تعتبر الجزائر من بين أكبر الدول من حيث استخدام الأوراق النقدية، مما يدل على وجود سيولة نقدية هائلة خارج البنوك لا تستغل اقتصاديا.

- غياب الإطار القانوني الخاص بالتجارة الإلكترونية، وعدم وضوح الجهة المسؤولة عن قطاع التجارة الإلكترونية في الجزائر.

وعليه لازالت التجارة الإلكترونية في بدايتها، مع الانتباه إلى عدم إغفال المخاطر التي يمثلها هذا النوع من التجارة. فوجود نظام للدفع الإلكتروني يستوجب على المشرع توفير إطارا متكاملا للحماية الجزائية والفنية له منعا للاعتداء عليه، وهذا ما سنراه لاحقا.

ثانيا: مفهوم نظام الدفع الإلكتروني وأدواته: لاشك أن هناك علاقة وطيدة بين الأشكال المختلفة للتجارة وتنوع طرق تسوية المعاملات الناتجة عن هذه التجارة، فكل شكل من أشكال التجارة يتمثل معه شكل من أشكال التسوية والدفع، وهو ما ينطبق أيضا على التجارة الإلكترونية[3]. ففي ظل

---

[1] المذكرة نفسها، ص230.

[2] تفاصيل الموضوع منشورة على الموقع الرسمي لوكالة الأنباء الجزائرية على الرابط الآتي: *http://www.aps.dz/ar/economie/34600-%D8%A7%D9%84%D8%A5%D8%B7%D9%84%D8%A7%D9%82-%D8%A7%D9%84%D8%B1%D8%B3%D9%85%D9%8A-%D9%84%D8%AE%D8%AF%D9%85%D8%A9-%D8%A7%D9%84%D8%AF%D9%81%D8%B9-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A*،تاريخ الاطلاع:2016/10/05 على الساعة:10:01.

[3] عصام عبد الفتاح مطر، المرجع السابق، ص68.

التطور التكنولوجي الحاصل في الخدمات المصرفية الحديثة، انتشرت أنظمة الدفع الإلكتروني في كافة دول العالم، والتي جاءت نتيجة الثورة التكنولوجية في مجال المعاملات المالية العالمية، حيث أصبحت لهذه المفاهيم أهمية بالغة نتج عنها صناعة مالية ومصرفية عالمية جديدة لها آثارها الإيجابية في جميع المجالات رغم السلبيات المسجلة. حيث صار بإمكان عملاء البنوك إجراء العمليات المصرفية من خلال شبكات الإتصال الإلكترونية سواء بين الزبون والشركة التجارية أو بين العميل وبنكه أو بين البنوك فيما بينها.

أ- **تعريف نظام الدفع الإلكتروني:** تعتبر شبكة الإنترنت البيئة التي تنمو فيها المعاملات الاقتصادية والتجارية عامة ومعاملات الدفع الإلكتروني خاصة، لذا عرفت سرعة انتشار هائلة باستعمال برامج الحاسوب وتبادل البيانات بين العملاء التي ترسل عبر شبكة الإنترنت أو عبر الوسائط الإلكترونية الأخرى، حتى وصل الأمر في بعض الدول المتقدمة كاليابان وكوريا الجنوبية إلى استغلال ميزات الهاتف الذكي*(SMART PHONE)* في القيام بالعمليات المصرفية. فظهور التجارة الإلكترونية وانتشارها تطلب وجود وسائل الدفع الإلكتروني، للدفع مقابل السلع والخدمات، ولهذا تعتبر بمثابة البنية الأساسية المالية لعالم الأعمال الحديث[1].

ويقصد بنظام الدفع الإلكتروني: "عمليات التحويل الإلكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر بالبنك الذي يوجد به حسابه، وذلك من خلال شبكة التسوية الإلكترونية"[2]. كما عرفها المشرع التونسي في الفصل الثاني من القانون رقم:2000-83 المؤرخ في 09 أوت 2000 المتعلق بالمبادلات والتجارة الإلكترونية على أنها:" العمليات التجارية التي تتم عبر المبادلات الإلكترونية"[3]، كما يعرف أيضا على أنه:" :"الدورة الإلكترونية المأمونة والسريعة لنقل الأموال من المشتري إلى البائع عبر المؤسسات المالية وبأقل تكلفة ممكنة "[4]، حيث تعطي بطاقة الدفع الإلكتروني أو بطاقة الائتمان[5] الحق للعميل في الحصول على السلع والخدمات عبر شبكة

---

1 محرز نورالدين ومريم صيد، نظام الدفع الإلكتروني ودوره في تفعيل التجارة الإلكترونية، الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر – عرض تجارب دولية –المركز الجامعي خميس مليانة الجزائر، يومي:26-27 أفريل 2011، ص14.

2 محمد أمين الشوابكة، المرجع السابق، ص193.

3 الفصل الثاني من القانون رقم:2000-83 المؤرخ في 09 أوت 2000 المتعلق بالمبادلات والتجارة الإلكترونية، الرائد الرسمي للجمهورية التونسية، العدد:64 المؤرخ في:2000/08/11، ص2084.

4 محرز نورالدين ومريم صيد، المرجع السابق، ص14.

5 هناك أنواع عديدة لبطاقات الائتمان نذكر منها:==

==- بطاقة الصرّاف الآلي *(ATM Card)* : تسمح للشخص بخصم مبلغ من حسابه الجاري مباشرة لدفعه إلى التاجر، ويمكن الحصول عليها بعد فتح حساب لدى البنك، حيث يقوم البنك بإصدار البطاقة للعميل وربطها بحركة الحساب ولا يستطيع العميل

الإنترنت[1]. كما حددت المادة (27) من القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية وسائل الدفع الإلكتروني مثل: الدفع بواسطة الوفاء أو التحويل الإلكتروني للأموال الناشئة عن العقود الإلكترونية، أو الدفع بواسطة النقود الإلكترونية...إلخ[2] .

وعليه يمكن التمييز بين نظاميين عالميين للدفع الإلكتروني، الأول يسمى بنظام الدفع بواسطة بطاقات الائتمان المؤمنة عبر شبكة الإنترنت، والثاني نظام الدفع المرتكز على النقود الإلكترونية المعروف بـ*(e-cash)*[3].

ب- أدوات الدفع الإلكتروني: وفرّت التقنية المتقدمة وسائل عديدة تستعمل في نظام الدفع الإلكتروني نذكر منها:

- **آلات الصرف الذاتي*(Automated Teller Machines):*** بدأ استخدامها سنة 1967 بأحد فروع بنك(باركلز) بالمملكة المتحدة حيث كانت تسمح فقط بخدمة السحب النقدي، حيث تعتمد

استخدامها سواء في عمليات سحب نقدي من أجهزة الصراف الآلي أو في عمليات شراء من خلال أجهزة نقاط البيع إلا إذا كان رصيد الحساب دائن.

- بطاقة الائتمان*(Crédit Card):* وهى البطاقة التي تصدرها البنوك للعملاء بالتعاون مع شركات الدفع الدولية مثل: "فيزا، ماستر كارد، أمريكان إكسبريس،... إلخ، حيث يستطيع حامل البطاقة استخدامها في إجراء عمليات سحب نقدي أو لدفع قيمة مشترياته من المحلات التجارية التي تقبل التعامل فيها، ومن ثم تسديد قيمتها لاحقاً، حيث يمكن للعميل إما تسديد إجمالي المبلغ أو تسديد الحد الأدنى.

- بطاقة القيد الائتمانية *(Debit Card)*: وهي البطاقة التي تصدرها البنوك للعملاء بالتعاون مع شركات الدفع الدولية مثل: "فيزا ماستر كارد، أمريكان اكسبريس... إلخ"، حيث يستطيع حامل البطاقة استخدامها في إجراء عمليات سحب نقدي أو لدفع قيمة مشترياته من المحلات التجارية التي تقبل التعامل فيها، وتختلف عن بطاقة الائتمان في أنها تتطلب قيام العميل بدفع كامل المبلغ المستحق عليه فور استلام كشف الحساب.

- البطاقات الذكية*(Smart Card):* تحتوي هذه البطاقات على معلومات صاحبها ويمكنها التخزين بسعة كبيرة تفوق البطاقات السابقة الذكر، حيث تحمل كل المعلومات والتفاصيل، ويختارها العميل للتعامل بها لما لديها من ميزات، كميزة الدفع الفوري وإمكانية تحويلها لحافظة نقود إلكترونية، راجع، محمد عمر الشويرف، التجارة الإلكترونية في ظل النظام العالمي الجديد، ط1، دار زهرة للنشر والتوزيع، عمان، الأردن،2013، ص ص116-119، وأيضا، أسامة أحمد المناعسة، جلال محمد الزغبي، صايل فاضل الهواوشة، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، دار وائل للنشر والتوزيع، الأردن، 2001، ص173.

[1] الشحات إبراهيم محمد منصور، المرجع السابق، ص ص113-114.

[2] المادة (27) من القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية الذي اعتمد بقرار مجلس وزراء العدل العرب رقم: 812/د25 بتاريخ 2009/11/19.

[3] *Alain Bensoussan, Internet, Op.Cit,p.127.*

على وجود شبكة من الاتصالات تربط فروع البنك الواحد لتصل إلى بيانات العميل فورا والتي تقدم خدمات متطورة في مجال صرف المبالغ النقدية كالسحب والايداع...إلخ[1].

- **البنوك المنزلية *(Home Banks)*:** في هذا النوع من البنوك يتم ربط جهاز الحاسوب للعميل بنظام الحاسب الآلي للبنك والذي أصبح يعرف فيما بعد باسم البنوك المنزلية، حيث يتم تحويل البيانات من حاسوب العميل إلى حاسب البنك أو العكس، وعليه يعمل الحاسوب الشخصي للعميل كمحطة طرفية لاستقبال الخدمات المصرفية كطباعة كشوف الحساب، وطلب الشيكات، وإرسال التعليمات الصادرة من العميل للبنك مثل: تجديد الودائع، والتحويل من حساب إلى آخر[2].
- **الوحدات الطرفية عند نقاط البيع *(Point and Salle)*:**وهي عبارة عن حاسبات آلية موجودة في المحلات والأسواق والمتاجر الكبرى والتي تكون على اتصال مباشر بالحاسب الآلي للبنك، حيث تجرى عمليات التحويل وإعادة التحويل عبر شبكة ونواة الإتصال المختلفة، بحيث يمكن إدخال قيمة مشتريات العميل لتخصم من رصيد حسابه مباشرة في البنك وإضافة القيمة إلى حساب المتجر في البنك نفسه[3].
- **بطاقة الائتمان المصرفية *(Credit-Card)*:** عرفها المشرع الجزائري بموجب نص المادة (543مكرر23) من (ق.ت.ج) التي تنص على: "تعتبر بطاقة الدفع كل بطاقة صادرة عن البنوك والهيآت المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل الأموال" فهي عبارة عن بطاقات بلاستكية تمنحها البنوك، تسمح لهم بشراء بضائع أو الحصول على خدمات من منافذ البيع أو الخدمات، شريطة أن يتم الدفع على فترات وفق نصوص العقد بين المصرف والعميل[4].

برغم إيجابيات نظم الدفع الإلكترونية، إلا أنها لا تخلو من مخاطر أمنية لكافة الأطراف المتعاملين بها، سواء للمستهلك أو للتاجر أو مصدر البطاقة، فقد يتم قرصنتها والتلاعب في بياناتها المخزنة وإفشاء أسرار العميل وانتهاك السرية بما يضر بحاملها...إلخ[5].

ج- وسائل الدفع الإلكتروني في الجزائر: تتميز أغلب وسائل الدفع المستعملة في النظام المصرفي الجزائري بالقدم وأغلبها لا تتناسب مع المتطلبات التكنولوجية الحالية، كما تقتصر وظيفتها

---

[1] عبد الرحيم وهيبة، تقييم وسائل الدفع الإلكترونية ومستقبل وسائل الدفع التقليدية في ظل وجودها، الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر - عرض تجارب دولية -المركز الجامعي خميس مليانة - الجزائر، يومي:26-27 أفريل 2011، ص03، راجع أيضا، رياض فتح الله بصله، جرائم بطاقة الائتمان، دار الشروق، القاهرة مصر، ط1، 1995، ص ص100-101.

[2] رياض فتح الله بصله، المرجع السابق، ص14.

[3] عصام عبد الفتاح مطر، المرجع السابق، ص73.

[4] محمد عمر الشويرف، المرجع السابق، ص116.

[5] المرجع نفسه، ص ص126-127.

في الغالب على سحب النقود من الصرّاف الآلي برغم وظائفها المتعددة في مجالات أخرى، وبرغم هذه الوضعية تبذل الدولة جهودا معتبرة قصد مواكبة التطورات التكنولوجية التي فرضها مجال التجارة الإلكترونية، لذا بدأت في تبني بعض وسائل الدفع الحديثة نذكر منها:

- **بطاقة السحب:** في إطار التفاعل مع المستجدات التي يفرضها الانتقال إلى اقتصاد السوق لا سيما وأن إصلاح النظام البنكي الجزائري وجعله مطابقا للمعايير الدولية، أضحى متطلبا يحتمه الانضمام لمنظمة التجارة العالمية *(OMC)*، حيث نصت المادة (66) من الأمر رقم:03-11 المؤرخ في 2003/06/26 المعدل والمتمم لقانون القرض على وضع وسائل الدفع تحت تصرف الزبائن[1]، كما نصت المادة (69) منه على أنه: " تعتبر وسائل الدفع كل الأدوات التي تمكن من تحويل أموال مهما يكن السند أو الأسلوب التقني المستعمل" . ذكرت المادة الوسائل المستعملة على سبيل المثال قصد استيعاب أية تقنية جديدة من تقنيات الدفع الإلكتروني. كما نصت المادة(543 مكرر 23) على استعمال الوسائل الإلكترونية المتعلقة بالمعاملات المالية كالسحب والدفع[2].

في الشأن نفسه نصت المادة (03) من الأمر رقم:05-06 المؤرخ في:2005/08/23 المتعلق بمكافحة التهريب على:"...تعميم وسائل استعمال الدفع الإلكتروني...". وهو اتجاه محمود من المشرع لاعتماد مفهوم موسع لنظام الدفع في المعاملات التجارية. وعليه بادرت البنوك إلى إنشاء بطاقات السحب الخاصة بها، وكان هدف المشرع هو تحديث وسائل الدفع للنظام المصرفي الجزائري وتطوير التعاملات النقدية بين المصارف، إضافة إلى تحسين الخدمة المصرفية وزيادة حجم التداول الإلكتروني للنقود.

- **البطاقة الائتمانية:** وهي عبارة عن بطاقات بلاستيكية مزودة بشريحة ذكية تمتلك قدرة عالية على التخزين وتحتوي على سجل البيانات والمعلومات والأرصدة والمصروفات المالية، لذلك سميت بدفتر الشيكات الإلكتروني وعلى درجة عالية بخصوص سلامة إجراء المعاملات المالية، حيث يتم الدفع على فترات بموجب اتفاق مسبق بين الزبون والجهة المصدرة للبطاقة مقابل تحصيل فوائد

---

[1] تنص المادة (66) من الأمر رقم:03-11 المؤرخ في 2003/06/26 المعدل والمتمم لقانون القرض على: "تتضمن العمليات المصرفية تلقى الأموال من الجمهور وعمليات القرض، وكذا وضع وسائل الدفع تحت تصرف الزبائن وإدارة هذه الوسائل"، (ج. ر) رقم:52 المؤرخة في:2003/08/27، ص11.

[2] تنص المادة (543مكرر) من (ق.ت.ج) على: "تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك والهيآت المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل الأموال. تعتبر بطاقة سحب كل بطاقة صادرة عن البنوك والهيآت المالية المؤهلة قانونا وتسمح لصاحبها فقط بسحب الأموال".

كما لا يستلزم بالضرورة وجود مبالغ مالية راهنة بحساب العميل حال استخدامه البطاقة لأن الجهة المصدرة تضمن الدفع ثم تحصّل هذه المبالغ من العميل في وقت لاحق[1].

يهدف المشرع الجزائري من وراء إصدار هذه النوع من البطاقات توحيد التقنيات المكونة للجهاز المصرفي قصد تبسيط استعمالها، وفي نفس الوقت وسيلة دفع مؤمنة بالنسبة للحامل ، حيث يتطلب ذلك تزويد مراكز المعالجة بمعدات وأجهزة طرفية، بالإضافة إلى تكوين لجنة من المصارف تمثل كل المشاركين لتحديد ووضع دليل للدفع الإلكتروني وقواعد التعامل بين التجار والعاملين ومعالجة قضايا عدم التسديد والنزاعات المختلفة، تمهيدا للانضمام لشبكات الدفع الدولية مثل:*(VISA)* أو *(Master Card)*. وبالفعل أصدرت الجزائر بطاقة "سي.بي.أ . فيزا. غولد" وهي عبارة عن بطاقة ائتمانية ترخصها هيئة عالمية "فيزا" وظيفتها إحلال عمولات إلكترونية بدل العملات التقليدية في الممارسة التجارية، وعن طريق هذه البطاقة يمكن لصاحبها شراء السلعة التي يرغبها على الإنترنت من أي مكان في العالم وتحويل الأموال إلى البائع عن طريق إرسال المعلومات البنكية عبر البريد الإلكتروني بشكل مشفر لضمان عدم قراءتها في حالة اعتراضها[2].

- **مركز معالجة النقدية ما بين المصارف:** تشرف شركة *(SATIM)* [3]على مركز المعالجة النقدية بين المصارف، وتعمل على ربط مراكز التوزيع مع مختلف المؤسسات المشاركة لوظيفة السحب، كما تقوم بتحديث نظام الدفع الإلكتروني من خلال استعمال البطاقة الإلكترونية وترقية التكنولوجيا في المجال البنكي. حيث يتولى هذا المركز ربط الموزع الآلي بمقدم الخدمة بواسطة خطوط عبر الشبكة الوطنية ومركز الاعتراض على البطاقات الضائعة أو المزورة، فعملية السحب تتم بطلب يوجه إلى مركز الترخيص بالوكالة الذي يقبله أو يرفضه، و في حالة القبول يراقب المركز السقف المسموح به أسبوعيا لكل زبون، كما يراقب الإشارة السرية، كما أن السحب الذي يتم بالبطاقة لا يمكن الرجوع فيه[4].

---

[1] رياض فتح الله بصله، المرجع السابق، ص29، راجع أيضا، عصام عبد الفتاح مطر، المرجع السابق، ص71، وسمية ديمش، المذكرة السابقة، ص ص242-243.

[2] زيدان زيبحة، المرجع السابق، ص39.

[3] أنشأت شركة تألية الصفقات البنكية المشتركة والنقدية *(satim)* في: 1995/03/25، وهي عبارة عن شركة مساهمة، يساهم في رأسمالها البنوك الجزائرية، من مهامها جمع مختلف ممثلي البنوك الوطنية والخاصة لتبادل المعلومات والتنسيق في عمليات السحب والدفع الخاصة بالموزعات الآلية للنقود *(ATM)*. في سنة 2007 تم تعميم استعمال بطاقة الدفع ما بين البنوك *(CIB)*، وما بين البنوك ومؤسسة البريد والمواصلات عبر كامل التراب الوطني، سمية ديمش، المذكرة السابقة، ص ص241-242.

[4] جميل أحمد ورشام كهينة، بطاقة الائتمان كوسيلة من وسائل الدفع في الجزائر، الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر – عرض تجارب دولية –المركز الجامعي خميس مليانة – الجزائر يومي:26-27 أفريل 2011، ص6.

الفرع الثاني: الحماية الجزائية والفنية لوسائل الدفع الإلكتروني:

كما قلنا سلفا لم يفرد المشرع الجزائري وسائل الدفع الإلكتروني بنصوص خاصة ضمن قانون العقوبات ولا بمناسبة تجريمه لأفعال المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون:04-15 المعدل والمتمم، لكن بالمقابل نص على ذلك بموجب نصوص خاصة مثل: البطاقة الإلكترونية التي يصدرها صندوق الضمان الاجتماعي بموجب قانون التأمينات الاجتماعية، من جانب آخر أضفى المشرع حماية فنية على وسائل الدفع الإلكتروني بهدف حماية المعاملات المالية التي تحدث في هذا الفضاء الافتراضي.

أولا: جرائم المساس بالبطاقات الإلكترونية بموجب قانون التأمينات: تماشيا مع توجهات المشرع الداعية إلى استعمال الوسائل الإلكترونية في عمليات الدفع الإلكتروني، جاء نظام الشفاء الذي يقوم على استعمال التكنولوجيات الدقيقة في إنتاج بطاقات ذات الشريحة تسمى" الشفاء "بهدف العصرنة الشاملة لمنظومة الضمان الاجتماعي في الجزائر، حيث أصدرت وزارة العمل والتشغيل والضمان الاجتماعي عن طريق الصندوق الوطني للتأمينات الاجتماعية للعمال الأجراء البطاقة الإلكترونية المسماة (بطاقة شفاء) *(Carte CHIFA)*بموجب القانون رقم:08-01 المؤرخ في:2008/01/23 يتعلق بالتأمينات الاجتماعية، حيث نصت المادة (06 مكرر) على: "تثبت صفة المؤمن له اجتماعيا ببطاقة إلكترونية..."، كما نصت المادة 65 مكرر على تزويد كل مقدم خدمة للعلاج بمفتاح إلكتروني[1]. كما نصت المادة(65 مكرر3) على إعداد وإرسال الفواتير إلكترونيا إلى هيئات الضمان الاجتماعي بغرض التعويض[2].وبهدف مكافحة الجرائم الإلكترونية الواقعة على الاستعمال غير المشروع لها نص في القانون نفسه من المادة(93 مكرر2 - 93 مكرر6) على هذه الجرائم والعقوبات المقررة لها، سنتطرق بإيجاز إلى هذه الجرائم حسب الركن الشرعي والمادي والمعنوي والعقوبات المقررة لها دون تكرار لشرح عناصر الركن المادي إذا تشابهت مع الركن المادي لجرائم المساس بأنظمة المعالجة الآلية للمعطيات التي تناولناها سابقا.

---

[1] تنص المادة (65 مكرر) من القانون رقم:08-01 على:" يزوّد كل مقدم علاج ، لاسيّما مستخدمو الصحة الذين يمارسون في الجزائر، بأي صفة كانت بمفتاح إلكتروني يسمى" المفتاح الإلكتروني لمهني الصحة".

[2] تنص المادة (65 مكرر3) من القانون رقم:08-01 على:" يتعيّن على مقدمي العلاج أو هياكل العلاج أو الخدمات المرتبطة بالعلاج، لاسيّما مستخدمو الصحة، استعمال البطاقة الإلكترونية للمؤمن له اجتماعيا مع مفاتيحهم الإلكترونية من أجل : قراءة وإدخال كل عمل وخدمة علاج أو خدمات مرتبطة بالعلاج المقدمة للمؤمّنين لهم اجتماعيا و/ أو ذوي حقوقهم – إعداد وإرسال الفواتير إلكترونيا إلى هيئات الضمان الاجتماعي بغرض التعويض ...".

أ- **جريمة الاستعمال غير المشروع للبطاقة الإلكترونية:**

1-الركن الشرعي: تنص المادة(93 مكرر2) من القانون رقم: 08-01 على:" دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 200.000 دج، كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمّن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة".

2-الركن المادي: يشتمل الركن المادي على العناصر الآتية:

- فعل التسليم: والمقصود هنا هو إعطاء البطاقة الإلكترونية أو المفتاح الإلكتروني لهيكل العلاج أو لمهني الصحة سواء من طرف أحد موظفي الجهة المصدرة للبطاقة مثل: الصندوق الوطني للضمان الاجتماعي *(CNAS)*، أو من طرف المؤمن له نفسه بقصد الاستعمال المخالف للقانون مثل: استعمال البطاقة الإلكترونية من قبل الغير في تعويض الأدوية باسم المؤمن له، وعادة ما يتم هذا الأمر بعلم وبموافقة المؤمن له، وقد كلف هذا الاستعمال غير المشروع أموالا ضخمة للصندوق الوطني للضمان الاجتماعي، مما دفع بالصندوق إلى اتخاذ إجراءات مشددة بخصوص المراقبة الطبية وآجال التداوي وعدد الوصفات والمبلغ المحدد...إلخ.
- فعل الاستلام: يكون من طرف الغير الذين لا يخول لهم القانون الاستفادة من خدمات الصندوق الوطني للضمان الاجتماعي.
- أن يكون الاستعمال مخالفا للقانون.

3-الركن المعنوي: جريمة عمدية تتطلب القصد الجنائي العام الذي يقوم على العلم والإرادة. فيجب أن يكون الجاني عالما بأن فعل التسليم والاستلام بهدف الاستعمال غير المشروع للبطاقة الإلكترونية أو المفتاح الإلكتروني يشكل جريمة معاقبا عليها قانونا، إضافة إلى اتجاه إرادة الجاني إلى القيام بالنشاط المجرّم.

4-العقوبات المقررة: دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 200.000 دج. حسب نص المادة (93مكرر2).

ب- **جريمة التلاعب في معطيات البطاقة الإلكترونية أو المفتاح الإلكتروني:**

1-الركن الشرعي: تنص المادة (93مكرر/1)على:" دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من

500.000دج إلى 1.000.000 دج ، كل من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية و/ أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمّن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة..." .

2-الركن المادي: و تشمل أفعال: التعديل أو المحو -شرحناها سابقا في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات- سواء جزئيا أو كليا للبيانات التقنية أو الإدارية مثل: اسم الهيئة المصدرة مدة الصلاحية، الحالة العائلية والاجتماعية للمؤمن له، حالات العلاج...إلخ. ويشترط أيضا أن تقع الجريمة على المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة، كما لا يشترط لقيام الجريمة إتيان الأفعال كلها، يكفي قيام الجاني بفعل واحد لتتحقق الجريمة.

3-الركن المعنوي: جريمة التلاعب في معطيات البطاقة الإلكترونية جريمة عمدية، تتطلب قصدا جنائيا عاما يقوم على علم الجاني بأن هذه الأفعال تشكل اعتداء على سلامة المعطيات داخل البطاقة أو المفتاح الإلكتروني وأنها ليست ملكا له، كما يجب أن تنصرف إرادته إلى ارتكاب هذه الأفعال، كما لا تتحقق الجريمة إلاّ إذا ارتكبت عن طريق الغش (العمد).

4-العقوبات المقررة: " دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 500.000 دج إلى 1.000.000دج ، وهذا حسب نص المادة (93 مكرر1/3).

ج- جريمة التلاعب في برمجيات البطاقة الإلكترونية أو المفتاح الإلكتروني:

1-الركن الشرعي: تنص المادة(93 مكرر2/3) على:"...يعاقب بنفس العقوبة، كل من أعد أو عدل أو نسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو استعمال المعطيات المدرجة في البطاقة الإلكترونية للمؤمّن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة... ".

2-الركن المادي: وتشمل أفعال: الإعداد، التعديل والنسخ:

-الإعداد: ويقصد به قيام الجاني ببرمجة أو تصميم برنامج معلوماتي بطريقة غير مشروعة قصد الوصول أو استعمال لمعطيات البطاقة الإلكترونية أو المفتاح الإلكتروني، تتطلب هذه العملية قدرا من المعرفة في مجال المعلوماتية وطرق البرمجة.

-**النسخ** : يتم تخزين البيانات المعالجة إلكترونيا في شكل نبضات كهربائية، وفي كل الحالات يمكن نسخها على أي دعامة تخزين[1].

3-الركن المعنوي: جريمة التلاعب في برمجيات البطاقة الإلكترونية أو المفتاح الإلكتروني جريمة عمدية تتطلب القصد الجنائي العام بعنصريه العلم والارادة، فيجب على الجاني أن يكون عالما بأن هذه الأفعال تشكل اعتداء على سلامة المعطيات داخل البطاقة أو المفتاح الإلكتروني، كما يجب أن تنصرف إرادته إلى ارتكابها، كما لا تتحقق الجريمة إلا إذا ارتكبت عن طريق الغش أي: العمد. كما يكفي لتحقق الجريمة قيام الجاني بفعل واحد من الأفعال السابقة.

4-العقوبات المقررة: تنص المادة (93مكرر1/3) على:" دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 500.000دج إلى 1.000.000 دج".

- **العقاب على الشروع:** عاقب المشرع على الشروع في هذين الجريمتين بموجب نص المادة 93 مكرر3 الفقرة الأخيرة:"... يعاقب بنفس العقوبة، على المحاولة في ارتكاب الجنح المذكورة في الفقرتين الأولى والثانية أعلاه".

د- جريمة الاتجار غير المشروع في البطاقة الإلكترونية أو المفتاح الإلكتروني:

1- الركن الشرعي: تنص المادة (93 مكرر4) على:" دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 500.000 دج إلى 5.000.000 دج كل من ينسخ أو يصنع أو يحوز أو يوزع بطريقة غير مشروعة البطاقة الإلكترونية للمؤمّن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة".

2- الركن المادي: ويتكون من أفعال:

-**النسخ:** ويقصد به قيام الجاني بطريقة غير مشروعة بإنجاز نسخة طبق الأصل عن البطاقة الإلكترونية أو المفتاح الإلكتروني الأصليين، وذلك باستعمال أدوات توفرها التكنولوجيا الحديثة.

-**الصنع:** توفر التكنولوجيا الحديثة إمكانيات هائلة بخصوص صناعة وتقليد المنتجات فيستطيع الجاني بطريقة غير مشروعة استعمال هذه الوسائل لصناعة بطاقة إلكترونية...إلخ.

-**الحيازة:** يقوم فعل الحيازة على امتلاك الجاني للبطاقة الإلكترونية أو المفتاح الإلكتروني بنية التملك ودون علم ورضا المالك.

---

[1] هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص235.

-**التوزيع:** يقوم الجاني بطريقة غير مشروعة بتوزيع البطاقة الإلكترونية أو المفتاح الإلكتروني بغير ترخيص من الجهة المعنية.

3-الركن المعنوي: هي جريمة عمدية تتطلب القصد الجنائي العام بعنصريه العلم والإرادة فيجب على الجاني أن يكون عالما بأن هذه الأفعال تشكل النشاط الجرمي المعاقب عليه قانونا، كما يجب أن تتصرف إرادته إلى ارتكاب هذه الأفعال، ويكفي قيام الجاني بفعل واحد حتى تتحقق الجريمة.

4-العقوبات المقررة: دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 500.000 دج إلى 5.000.000دج.

هـ- عقوبة الشخص المعنوي: إذا ارتكبت هذه الجرائم من طرف الشخص المعنوي تنص المادة(93 مكرر5) على:" يعاقب كل شخص معنوي يرتكب إحدى الجنح المنصوص عليها في المادة 93 مكرر3 و93 مكرر 4 أعلاه بغرامة تساوي خمس (5) مرات المبلغ الأقصى للغرامة المقررة للشخص الطبيعي".

و- العقوبات التكميلية: مع استبعاد الغير حسن النية وعدم علم المالك، تنص المادة (93 مكرر6) على:" دون الإخلال بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والوسائل المستعملة وكذا غلق المحلات وأماكن الاستغلال التي تكون محل الجنح المنصوص عليها في المادتين 93 مكرر 3 و 93 مكرر 4 أعلاه ، في حالة ما إذا كان المالك على علم بذلك ".

يلاحظ أن المشرع الجزائري شدّد من العقوبات على هذه الجرائم نظرا لخطورتها، وبقصد توفير الحماية الجزائية لوسائل الدفع الإلكترونية التي هي أساس التجارة الإلكترونية. وهو مسلك حسن يتماشى والتطورات التكنولوجية الحاصلة في مجال تقنية المعلومات. برغم ذلك لم يكتف المشرع بهذه النصوص وأضفى حماية فنية أخرى لا تقل أهمية عن الحماية الجزائية، سنتعرف عليها في الفرع الموالي.

ثانيا: الحماية الفنية لوسائل الدفع الإلكتروني: مع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يعرف بنقل البيانات عبر الشبكة من موقع لآخر، أصبح النظر إلى أمن تلك البيانات والمعلومات أمرا في غاية الأهمية، خاصة أن استعمال هذه الوسائل يتم في عالم المال والأعمال بما ينعكس إيجابا على تطور اقتصاد الدول، وإدراكا من المشرع الجزائري

بأهمية الدور الذي تلعبه وسائل الدفع الإلكتروني، سارع إلى إضفاء حماية تقنية، إضافة إلى الحماية الجزائية بهدف قطع الطريق على الإجرام الإلكتروني في مجال التعاملات المالية الإلكترونية. سنتعرف على بعض صور هذه الحماية كما يأتي:

1- تنظيم بنك الجزائر : أصدر بنك الجزائر تنظيم رقم:05-07 المؤرخ في:2005/12/28 يتعلق بأمن أنظمة الوفاء، وهو عبارة عن جملة من الإجراءات الوطنية والدولية بين البنوك والمؤسسات المالية المنخرطة في غرفة المقاصة. حيث فرض البنك على كل عضو في هذا النظام اتخاذ الإجراءات اللاّزمة بمعايير نظام المواكبة للقواعد الدولية في هذا المجال. حيث تقوم أنظمة الدفع على ضمان البنية التحتية للنظام ووسائل الدفع المختلفة كالتجهيزات التقنية ومدى نجاعتها خاصة ما تعلق بالاتصالات والطاقة الكهربائية[1]. في نفس الصدد نصت المادة (05) منه على أمن المنشآت والأنظمة مثل: جاهزية الأنظمة، تثبيت المعلومات المتبادلة، السرّية، إمكانية المراقبة، وترك آثار المعلومات المتبادلة...إلخ[2].

2- الإثبات بالكتابة في الشكل الإلكتروني: نصت المادة (323 مكرر 1) من (ق.م.ج) على: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها". وبذلك انتقل المشرع الجزائري من الاثبات بالورق إلى الاثبات بالكتابة في الشكل الإلكتروني ضمن قواعد الاثبات في القانون المدني. كما بين في المادة (323 مكرر) من (ق.م.ج) على: "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها"، ويتحدث المشرع هنا عن كافة الوسائل الإلكترونية المستعملة مثل: القرص الصلب أو المرن، أو الذاكرة الوميضية ...إلخ والمثبتة على دعائم غير ورقية، وأيضا باستعمال أي طريقة للإرسال مثل: البريد الإلكتروني...إلخ.

وعليه اعتبر المشرع الجزائري الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط التأكد من هوية الشخص الذي اصدرها وهو مما لا يخلق أي تعارض بخصوص حجية الإثبات، وهو يشكل حماية تقنية لوسائل الدفع الإلكتروني في حال تعلق الأمر بإثباتها.

3- التوقيع الإلكتروني: لقد عمدت أغلب التشريعات المقارنة التي نظمت التوقيع الإلكتروني إلى وضع تعريف له، وإزالة الغموض عن هذا المصطلح القانوني الحديث. فهو عبارة عن:" معلومات على شكل إلكتروني متعلقة بمعلومات إلكترونية أخرى ومرتبطة بها ارتباطاً وثيقاً ويستخدم أداة

---

[1] المادة (04) من نظام بنك الجزائر رقم:05-07 المؤرخ في:2005/12/28.

[2] المرجع نفسه، المادة (05) .

للتوثيق"[1]، وبإدراج المشرع الجزائري نظام الإثبات بالكتابة في الشكل الإلكتروني ضمن قواعد الإثبات، وتبعا لمتطلبات المعاملات الإلكترونية لاسيما في مجال التجارة الإلكترونية ، وفي ظل التوجه نحو الحكومة الإلكترونية، عرّف المشرع التوقيع الإلكتروني بموجب المادة (02) من القانون رقم:15-04 المؤرخ في:2015/02/01 على أنه:" بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق"، كما نصت المادة (03 مكرر) من المرسوم التنفيذي رقم: 07-162 المؤرخ في:2007/05/30 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاّسلكية الكهربائية، على شروط التوقيع المؤمن منها أن يكون خاصا بالموقّع وانشائه بوسائل يمكن أن يحتفظ بها الموقع[2]. كما يتطلب حماية التوقيع الإلكتروني ضرورة وجود مفتاح للتشفير الخاص وآخر للتشفير العام نصت عليهما المادتان(08 -09) من القانون رقم:15-04 سالف الذكر.

إن الهدف الأساس من إقرار التوقيع الإلكتروني والاعتراف بحجيته في الاثبات، هو توفير الحماية اللاّزمة لوسائل الدفع الإلكتروني بالنسبة لمعاملات التجارة الإلكترونية وزرع الثقة لدى المتعاملين لما يمتاز به من مستوى عال للسرّية والخصوصية، فهو يقوم على استخدام تقنية المعلومات كالتشفير والترقيم، وهو لا ينتج أي حجية قانونية ما لم يكن موثقاً بحسب الشروط القانونية[3].

4- القانون رقم:09-04: نصت المادة (01) من القانون رقم:09-04 المؤرخ في:2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على:" يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ".جاء هذا القانون ليوضح الإجراءات الخاصة للوقاية من الجرائم الإلكترونية بكافة أشكالها ومنها التي تقع على وسائل الدفع الإلكتروني.

المطلب الثالث: جرائم تقليد المصنفات المعلوماتية بموجب قانون حقوق المؤلف

[1] سعيد السيد قنديل، التوقيع الإلكتروني، ماهيته –صوره–حجيته في الإثبات، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ط2 2006، ص60.

[2] تنص المادة (03 مكرر) على:" هو توقيع إلكتروني يفي بالمتطلبات الآتية : يكون خاصا بالموقّع – يتم إنشاؤه بوسائل يمكن أن يحتفظ بها الموقّع تحت مراقبته الحصرية ... بحيث يكون كل تعديل لاحق للفعل قابلا للكشف عنه"، المرسوم التنفيذي رقم:07–162 المؤرخ في:2007/05/30 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاّسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاّسلكية، (ج. ر) رقم:37 المؤرخة في:2007/07/07، ص13.

[3] عبد الفتاح بيومي حجازي، النظام القانوني، المرجع السابق، ص114.

تماشيا مع الحركة التشريعية العالمية التي اهتمت بحماية البرمجيات عن طريق حقوق الملكية الفكرية والأدبية منذ اتفاقية باريس لسنة 1883، أصدر المشرع الجزائري الأمر رقم: 05/03 المؤرخ في 2003/07/19 يتعلق بحقوق المؤلف والحقوق المجاورة، اعتبر فيه برامج الحاسوب وقواعد البيانات من المصنفات الأدبية والفنية الجديرة بالحماية-تطرقنا إلى هذا الموضوع في الفصل الأول- سنتناول جنحة تقليد المصنفات المعلوماتية، والتي تمس بالحقوق المعنوية والمادية للمؤلف والعقوبات المقررة لها في (الفرع الأول)، ثم نتطرق إلى الجرائم المشابهة لجنحة التقليد، وكذا الاشتراك في المساس بحقوق المؤلف ورفض دفع المكافأة المستحقة في(الفرع الثاني).

الفرع الأول: جنحة تقليد المصنفات المعلوماتية الماسة بالحق المعنوي والمالي للمؤلف:

يقصد بالمصنف: "كل منتج ذهني أو فكري أيا كانت الصورة المادية التي يبدو فيها وبغض النظر عن نوعه أو أهميته أو الغرض من وضعه أو طريقة التعبير عنه"[1]، كما لا يعتد بنوع المصنف ولا بطريقة عرضه سواء كان مصنفا أدبيا أو علميا أو فنيا ومنها برامج الحاسوب.

تعد جريمة تقليد المصنفات المعلوماتية من أكثر الجرائم انتشارا في ظل تكنولوجيا تقنية المعلومات وما توفره من إمكانات تتيح للمجرم الإلكتروني القيام بكافة الأفعال المشكلة للجريمة كنسخ برمجيات الحاسوب والاتجار في نسخ مقلدة...إلخ. يمكن تعريف جريمة التقليد على أنها: "نقل مصنف لم يسقط في الملك العام من غير إذن مؤلفه" أو هي: "كل اعتداء يقع على الملكية الأدبية وأنه لابد من توافر شرطين أساسيين هما: وجود سرقة أدبية كلية أو جزئية للمصنف، وأن يتسبب هذا الاعتداء في ضرر"[2].

أولا: أركان جنحة التقليد: تتمثل في:

1-الركن الشرعي: تنص المادة (151/2-1)على: "يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية:

- الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف.
- استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة..."

---

[1] محمد أمين الرومي، المرجع السابق، ص77.

[2] أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت، المرجع السابق، ص ص144-145.

كما تنص المادة (152) من القانون نفسه على:" يعد مرتكبا لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الأداء عن طريق التمثيل أو الأداء العلني، أو البث الإذاعي السمعي أو السمعي البصري، أو التوزيع بواسطة الكابل أو بأية وسيلة نقل أخرى لإشارات تحمل أصواتا أو صورا وأصواتا أو بأي منظومة معالجة معلوماتية".

2- الركن المادي: يتمثل في أفعال:

-**الكشف غير المشروع للمصنف:** أجاز المشرع لصاحب المصنف المعلوماتي وحده الكشف عنه بالتاريخ والطريقة التي يراها مناسبة، عكس ذلك يعتبر إذاعة ونشر هذا المصنف اعتداء على حق صاحب المصنف.

-**الاعتداء على الحق في سلامة المصنف:** في هذا الشأن نصت المادة (25) من الأمر03-05 على:" يحق للمؤلف اشتراط احترام سلامة مصنفه والاعتراض على أي تعديل يدخله عليه أو تشويه أو إفساده إذا كان ذلك من شأنه المساس بسمعته كمؤلف أو بشرفه أو بمصالحه المشروعة" وعليه لصاحب المؤلف حق الاعتراض على تعديل أو محو أو تغيير أو تشويه يقع من طرف الغير ويمس بسمعة وشرف ومصالح المؤلف وهذا بدون علمه مثل: شراء شخص لبرنامج حماية لحاسوبه الخاص ثم بعد ذلك يقوم بتثبيته في حاسوب شخص آخر مجانا، وبذلك يمس بمصالح مالية مشروعة للمؤلف.

-**الاعتداء على حق النسخ:** يمكن تعريف القرصنة على أنها: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحوله عن طريقه"[(1)]، كما تعرف أيضا على أنها: "نشاطات تصنيع نسخ غير مصرح بها من المادة المحمية وتداول مثل هذه النسخ عن طريق التوزيع والبيع"[(2)]. وعليه يتحقق الاعتداء على حق المؤلف بنسخ المصنف المعلوماتي على دعامات معلوماتية بعدد فائض عن العدد المتفق عليه، سواء كان النسخ جزئيا أو كليا، كما تتحقق الجريمة سواء تم نسخ البرنامج باسم مؤلفه الحقيقي أو باسم خيالي والعبرة في تقدير وجود جنحة التقليد بأوجه الشبه لا بأوجه الاختلاف وتترك مسالة التقدير لمحكمة الموضوع[(3)].

-**الاعتداء على حق المؤلف في إبلاغ المصنف أو الأداء للجمهور:** وذلك باستعمال التمثيل أو الأداء العلني أمام الجمهور أو باستعمال الوسائل السمعية البصرية كالراديو والتلفزيون، شبكة الإنترنت، أو بأي وسيلة أخرى لبث الصوت والصورة أو باستعمال النظام المعلوماتي. بالمقابل أغفل

---

[1] محمود محمد لطفي صالح، المرجع السابق، ص212، راجع أيضا، هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص31.

[2] داريل بانثيير، المرجع السابق، ص2.

[3] علي عبد القادر القهوجي، المرجع السابق، ص ص31-32.

المشرع الاعتداء الواقع على تحويل المصنف وذلك بترجمته من لغة إلى أخرى مثل: الترجمة من لغة كوبول إلى لغة فوتران[1].

- **عدم ترخيص المؤلف:** تتحقق الجريمة بعدم وجود إذن كتابي من صاحب المؤلف أو ممن ينوبون عنه أو من الجهة التي تمتلك حقوق التأليف[2].

3- الركن المعنوي: تقوم هذه الجرائم على القصد الجنائي العام بعنصريه العلم والإرادة فيجب أن يكون مرتكبا جنحة التقليد عالما بأن صور النشاط الجرمي سابقة الذكر، أفعال معاقب عليها قانونا، إضافة إلى اتجاه إرادته للقيام بها. إن حسن النية هنا غير مفترض بدليل نص المشرع في المادة (151) سالفة الذكر على:" :"يعد مرتكبا لجنحة التقليد..." وهي مسألة تقديرية تترك لمحكمة الموضوع.

ثانيا: العقوبات المقررة:

1- العقوبات الأصلية: الحبس من (6) أشهر إلى (3) سنوات وبغرامة من خمسمائة ألف دينار (500.000دج) إلى مليون دينار(1.000.000دج) سواء كان النشر قد حصل في الجزائر أو في الخارج. وهذا حسب نص المادة (153) من الأمر 03-05 سالف الذكر.

2- حالة العود: نصت المادة (156) من الامر03-05 على: "تضاعف في حالة العود العقوبة المنصوص عليها في المادة (153) من هذا الأمر" كما قررت المادة نفسها الفقرة(2) على إمكانية غلق مؤسسة المقلّد أو الشريك مدة لا تتعدد 6 أشهر أو الغلق النهائي عند الاقتضاء.

3- العقوبات التكميلية: نصت المادة (157) من الأمر نفسه على: "تقرّر الجهة القضائية المختصة مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء. مصادرة واتلاف كل عتاد أنشئ خصيصا لمباشرة النشاط غير المشروع وكل النسخ غير المقلدة". كما نصت المادة (159) من الأمر03-05 على:" تأمر الجهة القضائية المختصة في جميع الحالات المنصوص عليها في المادتين 151 و152 من هذا الأمر بتسليم العتاد أو النسخ المقلدة أو قيمة ذلك كله وكذلك الإيرادات أو أقساط الإيرادات موضوع المصادرة للمؤلف أو لي مالك حقوق آخر أو طوي حقوقهما لتكون عند الحاجة بمثابة تعويض عن الضرر اللاّحق بهم".

---

[1] أمال قارة، المرجع السابق، ص87.

[2] حنان ريحان مبارك المضحكي، المرجع السابق، ص175.

ثالثا: العقاب على الاشتراك: نصت المادة (154) من الأمر نفسه على تطبيق العقوبات المنصوص عليها بموجب المادة (153) على الشخص الذي يشارك في الجنح المنصوص عليها في المادة (151) بعمله أو بالوسائل التي يحوزها مثل: الحاسوب وملحقاته...إلخ.

الفرع الثاني: الجرائم المشابهة لجنحة التقليد: تتمثل في جريمة التعامل في البرامج المقلدة وجريمة رفض دفع المكافأة المستحقة للمؤلف.

أولا: جريمة التعامل في البرامج المقلدة:

1-الركن الشرعي: تنص المادة (5/4/3/151) من الأمر 03-05 على: " يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية"...استيراد أو تصدير نسخ مقلدة من مصنف أو أداء. بيع نسخ مقلدة لمصنف أو أداء. تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو أداء".

2- الركن المادي: يتكون الركن المادي من صور التعامل المجرمة في البرامج المقلدة سواء قُلّدت داخل الوطن أو خارجه، فعملية التقليد تنصب على استيراد أو بيع أو تأجير البرمجيات بطريقة غير شرعية بما في ذلك البيع تحت علامات تجارية مزيفة[1].

3- الركن المعنوي: تقوم هذه الجرائم على القصد الجنائي العام بعنصريه العلم والإرادة، وعليه يكون الجاني عالما بأن صور التعامل في برامج مقلدة تشكل أفعالا جرمية معاقب عليها قانونا إضافة إلى اتجاه إرادته للقيام بهذه الأفعال، مع ملاحظة توفر القصد الجنائي الخاص ممثلا في قصد الاستغلال التجاري في حالتي استيراد وتصدير نسخ لبرامج مقلدة أو بيع وتأجير نسخ مقلدة، وبالتالي من يدخل البرنامج للاستعمال الشخصي لا يتوفر في حقه الركن المعنوي[2].

4- العقوبات المقررة: الحبس من (6) أشهر إلى (3) سنوات وبغرامة من خمسمائة ألف دينار (500.000دج) إلى مليون دينار(1.000.000دج) وهذا حسب نص المادة (153) من الأمر 03-05، إضافة إلى العقوبات التكميلية سالفة الذكر.

ثانيا: جريمة رفض دفع المكافأة المستحقة للمؤلف: يعتبر كل شخص رفض تسليم المكافأة المستحقة للمؤلف أو لأي مالك حقوق مجاورة مرتكب لجنحة التقليد وهذا بموجب نص المادة (155) من الأمر نفسه، ويعاقب بالعقوبات المنصوص عليها بموجب المادة (153) سالفة الذكر[3]. وهذا ضمانا للحقوق المكتسبة للأفراد.

---

[1] حنان ريحان مبارك المضحكي، المرجع السابق، ص173.

[2] أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت، المرجع السابق، ص150.

[3] المادة (155) من الأمر رقم:03-05 يتعلق بحقوق المؤلف والحقوق المجاورة.

المطلب الرابع: الجرائم الماسة بالتوقيع الإلكتروني بموجب القانون15-04

تتوجه الجزائر تدريجيا نحو تحقيق متطلبات الحكومة الإلكترونية بما يصاحبها من تحديات كبيرة، سواء على مستوى توفير الإطار القانوني أو على مستوى توفير الامكانات والوسائل التقنية والتكنولوجيا المتطورة وعلى رأسها توفير خدمات شبكة الإنترنت ذات التدفق العالي. وتلعب التجارة الإلكترونية رغم مخاطرها العديدة دورا بارزا في مجال تطوير الاقتصاد الرقمي بما يسهل المعاملات المالية باستعمال وسائل الدفع الإلكتروني. في هذا الصدد ونتيجة للحاجة الملحة لأمن المعلومات والحفاظ على الخصوصية على شبكة الإنترنت وزيادة الثقة بين المتعاملين في هذا الفضاء الافتراضي، يواصل المشرع الجزائري بناء المنظومة القانونية للحكومة الإلكترونية في شتى المعاملات سواء كانت تجارية أو مدنية، وذلك بالنص على التوقيع والتصديق الإلكترونيين بموجب القانون رقم: 15-04 المؤرخ في:2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، سنتطرق إلى ماهية التوقيع الإلكتروني في (الفرع الأول)، ثم إلى الجرائم الإلكترونية الواقعة عليه في (الفرع الثاني).

الفرع الأول: ماهية التوقيع الإلكتروني:

بسبب حداثة وغموض هذا المصطلح، وبهدف التأكيد على أهمية هذه الوسيلة في التعاملات المختلفة على شبكة الإنترنت، تعددت التعاريف التي أعطيت للتوقيع الإلكتروني بحسب النظم القانونية المختلفة، نتطرق للبعض منها كما يأتي:

أولا: تعريف التوقيع الإلكتروني: عرف التوقيع الإلكتروني في القانون العربي النموذجي الموحد على أنه:" بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو متصلة بها منطقيا يجوز أن نستخدم لتعيين هوية الموقّع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقّع على المعلومات الواردة في رسالة البيانات"[1]. كما عرفه أيضا قانون الاتحاد الأمريكي على أنه:" صوت أو رمز أو معالجة إلكترونية مرفقة أو متحدة بعقد أو بغيره من السجلات يتم تنفيذها أو اقرارها من شخص تتوافر لديه نية التوقيع على السجل[2]. كما عرفه المشرع المصري بموجب المادة (01) من مشروع قانون التجارة الإلكترونية لسنة2001 على أنه: "حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتميزه عن غيره"[3].

1 عبد الفتاح بيومي حجازي، نحو صياغة، المرجع السابق، ص71.

2 أشرف توفيق شمس الدين، المرجع السابق، ص46

3 عصام عبد الفتاح مطر ، المرجع السابق، ص196.

من جهة أخرى اعتبر المشرع الفرنسي أن التوقيع الإلكتروني يدل على شخصية الموقّع، كما يضمن علاقته بالواقعة المنسوبة إليه وكذا صحتها إلى غاية ثبوت العكس[1]. كما عرفه آخرون على أنه: "يتم التوقيع الإلكتروني باستعمال وسائل مؤمنة وتضمن العلاقة بين الموقع والمستند الإلكتروني الذي يرتبط به"[2]. وعليه يعتبر التوقيع الإلكتروني وسيلة تسمح بضمان الصلة بين المنظومة العمومية للتشفير وصاحبها، بحيث يتأكد الطرف المتعامل بأن التوقيع المعين يتعلق بهوية الشخص المراد التعامل معه دون آخر، فيتحقق بذلك الأمان المطلوب[3].

لم يخرج المشرع الجزائري عن التعريفات السابقة، وعرّف التوقيع الإلكتروني بموجب (1/02) من القانون 15-04 سالف الذكر على أنه:" بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق". وهو التعريف نفسه الذي جاءت به نص المادة (1/02) من التوجيه الأوروبي رقم:99/93 المؤرخ في:1999/12/13 على أنه:" المعطيات التي تأخذ الشكل الإلكتروني والتي ترتبط بمعطيات أخرى إلكترونية تستخدم كوسيلة لإثبات صحتها"[4].من جانب آخر يعتبر التوقيع الإلكتروني مماثلا للتوقيع المكتوب، وذلك بنص المادة (08) من القانون 15-04 التي تنص على:" يعتبر التوقيع الإلكتروني الموصوف وحده مماثلا للتوقيع المكتوب سواء كان لشخص طبيعي أو معنوي" بشرط أن تتوافر في التوقيع الإلكتروني شروط قانونية حددها المشرع والتي سنتطرق إليها لاحقا.

من جانب آخر اعتبر المشرع الجزائري التوقيع الإلكتروني، تلك المعطيات التي تكون في شكل إلكتروني في صورة حروف أو أرقام أو رموز أو إشارات سواء كانت مرفقة بالسند الإلكتروني أو مرتبطة ارتباطا منطقيا بمعطيات إلكترونية أخرى، بهدف استعماله في توثيق المعاملات على اختلافها وبالتالي يعبر المشرع عن وجهة نظر فنية باعتباره وسيلة تكنولوجية لتحقيق الأمان والسرية[5]. وبهذه الصورة فالتوقيع الإلكتروني "يقلل بشكل كبير من احتمالات التزوير بسبب تطور

---

1 *David FOREST et Gautier Kaufman,Op.cit,p.84.*

2 *ADEL BRAHMI, Signature électronique et Droit, édition MS, Tunisie, 2004, p.15.*

3 إقلولي أولدرابح صافية، القوة الثبوتية لشهادات التصديق الإلكتروني في التشريع المقارن، ملتقى وطني حول:" الإطار القانوني للتوقيع والتصديق الإلكترونيين في الجزائر"، كلية الحقوق والعلوم السياسية، جامعة محمد الشريف مساعدية، سوق أهراس، الجزائر، يومي:16 و17 فيفري2016، ص3، راجع أيضا، . *Alain Bensoussan, Internet, Op.Cit,p.127*

4 التوجيه الأوربي رقم 1999/93 بشان الإطار المشترك للتواقيع الإلكترونية الصادر بتاريخ 1999/12/13.

5 سعيد السيد قنديل، المرجع السابق، ص60.

وسائل التخزين المعلوماتي"[1]، كما أن للتوقيع الإلكتروني أشكالا[2] متعددة أفرزها تنوع المعاملات الإلكترونية مثل: التوقيع الخطي، التوقيع الرقمي، واستخدام بطاقات الائتمان الممغنطة.

ثانيا: شروط التوقيع الإلكتروني: نصت المادة (07) من القانون رقم:15-04 على:" التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية:

- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.
- أن يرتبط بالموقّع دون سواه .
- أن يمكن من تحديد هوية الموقّع .
- أن يكون مصمّما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.
- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقّع.
- أن يكون مرتبطا بالبيانات الخاصة به بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات.

نستنتج من نص المادة الشروط القانونية الواجب توافرها في التوقيع الإلكتروني الموصوف نلخصها كما يأتي:

1-أن يكون متميزا ومرتبطا بصاحبه: يجب أن يكون التوقيع الإلكتروني علامة مميزة لشخصية الموقع، فالتوقيع بالخصائص الذاتية للشخص، وكذلك التوقيع بالقلم الإلكتروني أو التوقيع الرقمي وغيرها تتضمن علامات مميزة للشخص عن غيره، ويستوي أن يكون شخصا طبيعيا أو معنويا بحسب

---

[1] *Alain Bensoussan, L'informatique, Op.Cit,p.449.*

[2] من أشكال التوقيع الإلكتروني:

- التوقيع بالقلم الإلكتروني: ويتم هذا التوقيع عن طريق قلم إلكتروني حسابي، يمكن عن طريقه الكتابة على شاشة الحاسب الآلي، وذلك باستخدام برنامج معين.
- التوقيع البيومتري: يقصد به التحقق من الشخصية عن طريق الخواص الطبيعية والفيزيائية والسلوكية الحيوية، ومن ذلك بصمة الأصبع ومسح قرينة العين وبصمة الشفاه والتوقيع الشخصي، ونبرة الصوت، وبصمة الأسنان، وبصمة صيوان الإذن، ووجه الشخص... إلخ.

- التوقيع الكودي (البطاقات الممغنطة): تستخدم هذه البطاقات في السحب النقدي من خلال بطاقات الصرف الآلي، والتي تُخوّل حاملها إمكانية سحب مبالغ نقدية من حسابه بحد متفق عليه بينه وبين البنك مُصدر البطاقة، حيث تحتوي هذه البطاقة على رقم سرّي لا يعرفه إلا صاحبها، والذي يخوله الدخول إلى حسابه وإجراء العمليات التي يريدها.

- التوقيع الرقمي: يقوم على فكرة الرموز السرية والمفاتيح غير المتناسقة (المفاتيح العامة والمفاتيح الخاصة)، ويعتمد هذا التوقيع على فكرة اللوغاريتمات والمعادلات الرياضية المعقدة من الناحية الفنية كإحدى وسائل الأمان التي يبحث عنها المتعاقدون، راجع، سعيد السيد قنديل المرجع السابق، ص ص66-72، وعبد الفتاح بيومي حجازي، النظام القانوني، المرجع السابق، ص ص119-128.

نص المادة (2/02) من القانون 15-04 التي تنص على:" الموقّع كل شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله". ويتم إثبات هذه الصلة بحصول الموقّع على شهادة التصديق الإلكتروني التي تحتوي على بيانات التحقق من التوقيع الإلكتروني والموقّع، وهذا بموجب المادة (7/02) من القانون نفسه[1].

2- التعرف على هوية الموقع: يتطلب هذا الشرط أن يكون التوقيع الإلكتروني قادرا على التعريف بشخصية الموقع، فالتوقيع بالرقم السري مثلا قادر على تحديد هوية الموقع، لأن الرقم السري لا يعرفه إلا صاحبه، والحال كذلك في التوقيع الرقمي إذ يُمكّن من تحديد هوية الشخص الموقع بأنه هو من انصرفت إرادته إلى إنشاء الالتزام عن طريق وسيلة التوقيع الإلكتروني[2]، وذلك باستعمال آلية التحقق من التوقيع الإلكتروني الذي يتمثل في جهاز أو برنامج معلوماتي معد لتطبيق بيانات التحقق منه حسب نص (4/02) من القانون15-04 سالف الذكر[3].

3- سيطرة الموقّع على منظومة التوقيع: إذ يتطلب أن يكون صاحب التوقيع الإلكتروني منفردا به، بحيث لا يستطيع أي شخص معرفة فك رموز التوقيع الخاص به أو الدخول عليه سواء عند استعماله لهذا التوقيع أو عند إنشائه، كما يجي أن تكون آليات انشاء التوقيع الإلكتروني موصوفة ومؤمنة، وفقا لنص المادتين(10 -11) من القانون رقم: 15-04 سالف الذكر[4].

4-ارتباط التوقيع الإلكتروني بالموقّع: لابد أن يكون التوقيع الإلكتروني متصلا اتصالا ماديا ومباشرا بالموقّع حتى يكون دليلا على إقراره بما ورد في المستند الإلكتروني، فالموقّع يستعمل مفتاح التشفير الخاص به، بحيث لا يستطيع أحد الاطلاع على مضمون المحرّر الإلكتروني، حيث نصت المادة (8/02) على مفتاح التشفير الخاص الذي هو عبارة عن سلسلة من الأعداد يحوزها الموقع

---

[1] تنص المادة (7/02) من القانون رقم:15-04 على:" شهادة التصديق الإلكتروني: وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني ولموّقع".

[2] زيدان زيبحة، المرجع السابق، ص40.

[3] تنص المادة (4/02) من القانون رقم: 15-04 على:" آلية التحقق من التوقيع الإلكتروني :جهاز أو برنامج معلوماتي معد لتطبيق بيانات التحقق من التوقيع الإلكتروني".

[4] تنص المادة (10) من القانون رقم:15-04 على:" يجب أن تكون آلية إنشاء التوقيع الإلكتروني الموصوف مؤمنة"، كما نصت المادة (11) من القانون نفسه على الآليات المؤمنة.

فقط[1] الذي يمتلك المفتاح الخاص، ناهيك عن ارتباط مفتاحه الخاص بمفتاح التشفير العمومي وبالتالي فإن المحرر يرتبط بالتوقيع على نحو لا يمكن فصله أو التعديل فيه إلا الموقّع نفسه.

5- وجود شهادة تصديق إلكتروني موصوفة: وهي وثيقة في شكل إلكتروني[2] ثبت الصلة ببيانات التحقق من التوقيع الإلكتروني والموّقع يمنحها مؤدو خدمات التصديق الإلكتروني[3] المرخصون قانونا بإصدار هذه الشهادة الإلكترونية، وهذا بموجب المادة (41) من القانون15-04 التي تنص على:" يكلف مؤدي خدمات التصديق الإلكتروني بتسجيل وإصدار ومنح وإلغاء ونشر وحفظ شهادات التصديق الإلكتروني، وفقا لسياسة التصديق الإلكتروني[4] الخاصة به التي وافقت عليها السلطة الاقتصادية للتصديق الإلكتروني".

بالنسبة لحجية شهادات التصديق الإلكتروني في الاثبات، وكما رأينا سلفا اعتبر المشروع الجزائري بموجب نص المادتين(323 مكرر - 323 مكرر1) من (ق.م.ج) على اعتبار الاثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها. وكذا المادة (2/327) التي تنص على:"...ويعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر1أعلاه" وبالتالي يكون المشرع الجزائري قد اعتمد نهج النظير الوظيفي فيما يتعلق بقبول الكتابة الإلكترونية وإزالة الشكوك حول القيمة القانونية لها[5]، مما لا يخلق أي تعارض بخصوص حجية الاثبات، وهو يشكل حماية تقنية لوسائل الدفع الإلكتروني في حال تعلق الأمر بإثباتها.

الفرع الثاني: الجرائم الواقعة على التوقيع الإلكتروني:

نظرا لأهمية هذه الوسيلة في التعاملات الإلكترونية، أحاطها المشرع في القانون رقم:15-04 بعقوبات جزائية، ومالية، وإدارية سنتناولها فيما يأتي:

---

1 تنص المادة (8/02) من القانون 15-04 على:" مفتاح التشفير الخاص هو : عبارة عن سلسلة من الأعداد يحوزها حصريا الموقّع فقط ، وتستخدم لإنشاء التوّقيع الإلكتروني ، ويرتبط هذا المفتاح بمفتاح تشفير عمومي"، كما نصت المادة (9/02) على مفتاح التشفي العمومي الذي هو عبارة عن:" سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني".

2 تنص المادة (7/02) من القانون 15-04 على:" شهادة التصديق الإلكتروني: وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع".

3 تنص المادة (12/02) من القانون 15-04 على:" مؤدو خدمات التصديق الإلكتروني: شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي...".

4 تنص المادة (15/02) من القانون 15-04 على:" سياسة التصديق الإلكتروني: مجموع القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الإلكترونيين".

5 إقلولي أولدرابح صافية، المداخلة السابقة، ص6.

أولا: جريمة التلاعب في بيانات التوقيع الإلكتروني:

1-الركن الشرعي: تنص المادة (68) من القانون 15-04 على:" يعاقب بالحبس من ثلاثة (3)أشهر إلى ثلاث (3) سنوات وبغرامة من مليون دينار (1.000.000دج) إلى خمسة ملايين دينار (5.000.000 دج) أو إحدى هاتين العقوبتين فقط، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير".

أ- الركن المادي: يتمثل الركن المادي في الأفعال التالية:

-**الحيازة:** وهي سلطة فعلية لممارسة الشخص على شيء تظهره بمظهر صاحب الحق وتتحقق الحيازة غير المشروعة بسيطرة الحائز على المعلومات واستغلالها، كما لا تقوم الحيازة إلا بالسيطرة الإرادية للجاني[1]. وعليه تترتب مسؤولية مؤدي خدمات التصديق الإلكتروني عن حيازة غير مشروعة لبيانات[2] التوقيع الإلكتروني ومهما كانت الوسيلة المستعملة في ذلك، تتمثل هذه البيانات حسب نص المادة (3/02) في الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموّقع لإنشاء التوقيع الإلكتروني على أساس أنهم هم من يقومون بتسجيل وإصدار ومنح وإلغاء ونشر وحفظ شهادات التصديق الإلكتروني حسب نص المادة (41) من القانون15-04.

-**الافشاء:** ويقوم فيه الجاني بإفشاء بيانات التوقيع الإلكتروني الخاصة بالغير بغض النظر عن الوسيلة التي بموجبها آلت اليه، وما يشكل ذلك من خطورة بحيث يقوم الجاني بتقديم هذه المعلومات لغيره الذي ليس له الحق في الاطلاع عليها[3]، بما يمثل انتهاك لسرية البيانات ويضر بأمنها وسلامتها ويفقد ثقة المتعاملين بالوسائل الإلكترونية.

-**الاستعمال:** إذا كان حيازة وافشاء بيانات التوقيع الإلكتروني الموصوف للغير مسألة خطيرة فإن الأخطر منها هو استعمالها بما يمس بأمن وسرية بيانات الموقّع، وأيضا المساس بعنصري الثقة والائتمان خاصة في مجال التعاملات المالية الإلكترونية مثل: استعمال بيانات الموقّع في إنشاء توقيع إلكتروني ومنه الحصول على شهادة التصديق الإلكتروني لاستعمالها بطريقة غير مشروعة.

-**تعلّق البيانات بالغير:** إن بيانات التوقيع الإلكتروني الموصوف يحوزها الموقّع حصريا كمفتاح التشفير الخاص به، وعليه لا يمكن للجهة المانحة لشهادة التصديق الإلكتروني مثل: السلطة الوطنية للتصديق الإلكتروني أو السلطة الحكومية للتصديق الإلكتروني، القيام بأفعال الحيازة والإفشاء والاستعمال غير المشروعين للبيانات الخاصة بالموقّع.

---

[1] رشيدة بوكر، المرجع السابق، ص286.

[2] عرفت المادة (3/02) من (إ.ع.م.ج.ت.م) البيانات على أنها:" كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات كالأرقام والحروف والرموز وما إليها...".

[3] عصام عبد الفتاح مطر، المرجع السابق، ص337.

2-الركن المعنوي: جريمة التلاعب في بيانات التوقيع الإلكتروني جريمة عمدية تتطلب توافر القصد الجنائي العام الذي يقوم على العلم والإرادة، وعليه يتعين علم الجاني بمكونات السلوك الجرمي المكون لهذه الجريمة والمتمثلة في: الحيازة والافشاء والاستعمال، كما يجب أن تتجه إرادة الجاني إلى إتيان القيام بالأفعال سابقة الذكر[1].

3-العقوبات المقررة: الحبس من ثلاثة (3) أشهر إلى ثلاث (3) سنوات وبغرامة من مليون دينار (1.000.000دج) إلى خمسة ملايين دينار (5.000.000 دج) حسب نص المادة (68) سالفة الذكر.

ثانيا: العقوبات المالية والإدارية: لم يكتف المشرع بالنص على عقوبات جزائية في حال المساس ببيانات التوقيع الإلكتروني، بل وسّع من نطاق العقاب إلى فرض عقوبات مالية تتراوح ما بين 200.000دج إلى 5.000.000دج وعقوبات إدارية كسحب الترخيص الممنوح له، وهذا بشأن مؤدي خدمات التصديق الإلكتروني في حالة الإخلال بأحكام دفتر الأعباء أو سياسة التصديق الإلكتروني الخاصة بهم، وذلك بموجب المادة (64) من القانون 15-04 سالفة الذكر[2].

ثالثا: عقوبة الشخص المعنوي: نصت المادة (75) من القانون15-04 على:" يعاقب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في هذا الفصل بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي".

لم تتوقف السياسة الجنائية للمشرع الجزائري عند حدود مكافحة الجرائم الإلكترونية بموجب قانون العقوبات وبعض القوانين الخاصة، بل امتدت هذه المرة لتشمل التصديق على (إ.ع.م.ج.ت.م) حيث يطرح التساؤل: ماهي الجرائم الجديدة التي جاءت بها هذه الاتفاقية والتي لم ينص عليها المشرع الجزائري؟ هذا ما سنتعرف عليه في المبحث الثالث.

المبحث الثالث: مواجهة الجرائم الإلكترونية بموجب الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

بعدما ألقينا الضوء على مكافحته للجرائم الإلكترونية بموجب قانون العقوبات وبعض النصوص الخاصة لم يكتف المشرع بذلك، وامتدت سياسته الجنائية هذه المرة إلى المكافحة على المستوى الدولي حيث صادقت الجزائر على (إ.ع.م.ج.ت.م)، إذ تعتبر هذه الاتفاقية خطوة عملاقة ومكسبا مهما

---

[1] المرجع نفسه، ص337.

[2] تنص المادة (64) من القانون رقم: 15-04 على:" في حالة عدم احترام مؤدي خدمات التصديق الإلكتروني أحكام دفتر الأعباء أو سياسة التصديق الإلكتروني الخاصة به والموافق عليها من طرف السلطة الاقتصادية، تطبق عليه هذه السلطة عقوبة مالية يتراوح مبلغها بين مائتي ألف دينار (200.000 دج) وخمسة ملايين دينار (5.000.000دج)...".

للدول العربية في مجال مكافحة جرائم تقنية المعلومات بكافة صورها، حيث جاء في ديباجتها: "إن الدول العربية الموقعة، ورغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعا منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وأخذا بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية...".

إنّ الهدف من الحديث عن هذه الاتفاقية ينبع من أهميتها البالغة، إضافة إلى رسم صورة واضحة حول معالم السياسة الجنائية للمشرع الجزائري المتعلقة بمكافحة الجرائم الإلكترونية على المستوى الخارجي، والتطرق بإيجاز لبعض الجرائم المنصوص عليها في هذه الاتفاقية، والتي لم يجرّمها المشرع بعدُ سواء في قانون العقوبات أو ضمن قوانين خاصة للتعريف بها وبأهميتها وبيان خطورتها. فالمشرع الجزائري تأخّر كثيرا في التصديق على الاتفاقية أي قرابة أربعة سنوات من تاريخ التوقيع إلى تاريخ التصديق، ولا نعلم بعد كم سيأخذ من الوقت لتعديل قانون العقوبات وقانون الإجراءات الجزائية لإدماج نصوص هذه الاتفاقية. إن هذا التأخر لا يتلاءم مع التطور التكنولوجي المستمر في مجال تكنولوجيات الإعلام والاتصال والانتشار الواسع لها واستعمالها من كافة فئات المجتمع، مما يساعد المجرم الإلكتروني على الإفلات من العقوبة.

وعليه سنتطرق إلى جريمة الاعتراض غير المشروع للبيانات في (المطلب الأول) ثم نتناول جريمة التزوير المعلوماتي في(المطلب الثاني) لنتعرف على جريمة الإباحية والجرائم المرتبطة بها في (المطلب الثالث)، ثم نكتشف بعدها أهم الجرائم المنظمة عبر الوطنية التي تستعمل تقنية المعلومات وسنتناول جريمتي غسيل الأموال والمخدرات المرتكبتين عبر الإنترنت في(المطلب الرابع).

المطلب الأول: الاعتراض غير المشروع للبيانات

توفر التكنولوجيا المتطورة وسائل تقنية يمكن من خلالها اعتراض الإشارات الكهرومغناطيسية المرسلة أو المستقبلة من مختلف الأجهزة الإلكترونية، ومنها الحواسيب بهدف الحصول غير المشروع على البيانات والمعلومات واستغلالها في ارتكاب جرائم إلكترونية. سنتناول مفهوم الاعتراض غير المشروع للبيانات في (الفرع الأول)، ثم نتطرق إلى وسائل الاعتراض غير المشروع في (الفرع الثاني).

الفرع الأول: مفهوم الاعتراض غير المشروع للبيانات:

ويقصد به: "رصد اشارات إلكترومغناطيسية في الأنظمة المعلوماتية أو تحليلها بغية استخراج المعلومات المفهومة أو المقروءة منها"[1]، كما نصت عليه (إ.أ.م.إ.م) بموجب المادة (03) التي تنص على:"...التنصت أو نقل البيانات التي تتم داخل جهاز الحاسب أو التي تتم عبر جهازين عن بعد عبر الشبكات المعلوماتية المختلفة أو بترجمة انبعاثات الكهرومنغاطيسية ...أو التي تتم عبر الأجهزة اللاسلكية وذلك عن طريق أي من الوسائل الفنية..."[2].تناولته أيضا المادة(07) من (إ.ع.م.ج.ت.م) على أنه:" الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات". كما أوضحت المذكرة التفسيرية (إ.أ.م.إ.م) أن تطبيق نص المادة(03) يمتد إلى كافة أشكال النقل الإلكتروني للبيانات سواء تم هذا النقل عن طريق التلفون أو الفاكس، أو البريد الإلكتروني أو نقل الملفات[3].

وكما أشرنا سابقا أن المشرع الجزائري لم يفرد فعل الاعتراض غير المشروع على البيانات المرسلة إلكترونيا أو المعلومات المرسلة عن طريق المنظومة المعلوماتية بموجب نص خاص، إلاّ أنه وسّع من مفهوم الاتصالات الإلكترونية ليشمل كل وسائل نقل المعلومات التي تتم بطريقة إلكترونية سواء داخل النظام نفسه أو بين مجموعة أنظمة متصلة فيما بينما وهذا بموجب نص المادة (02/و) من القانون رقم:09-04 السابق ذكره على أنها:" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية." لكنه بالمقابل نص على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، بموجب المادة(65 مكرر5 – 65 مكرر10) من القانون رقم:06-22 المؤرخ في 2006/12/20 المعدل والمتمم لقانون

---

[1] رشيدة بوكر، المرجع السابق، ص205.

[2] ***Article 3 – Interception illégale***

"Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.", convention européenne de la cybercriminalité, Op.Cit,p.3.

[3] المذكرة التفسيرية لاتفاقية بودابست للإجرام المعلوماتي منشورة على موقع الاتحاد الأوروبي على الرابط الآتي: *http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ccea4,p11* ، *تاريخ الاطلاع: 2015/12/21 : الساعة: 09:56.*

الإجراءات الجزائية ، تناول فيها سلطة تقدير اللجوء إلى اعتراض المراسلات وأطر التحقيق الممارس فيها وأنواع الجرائم التي تستعمل فيها تقنية اعتراض المراسلات وشروط الإذن باعتراض المراسلات الشكلية ومضمونه ومدته...إلخ، والذي سنتطرق إليه في الفصل الثاني بخصوص أساليب التحري الخاصة في الجرائم الإلكترونية .

نستنتج من التعاريف السابقة أن فعل الاعتراض يمكن أن يقع داخل منظومة معلوماتية واحدة أو بين نظامين متصلين سواء بشبكة داخلية *(INTARNET)*[1]، أو عن طريق شبكة الإنترنت كما هو الشأن في البريد الإلكتروني، إذ يغطي النظام المعلوماتي كافة أنواع الاتصالات الإلكترونية مثل: شبكة *(wifi)* وهي نظام مفتوح من السهل اعتراضه باستعمال وسائل إلكترونية. ويتم ذلك عن طريق اعتراض خط سير البيانات الإلكترونية أو قطع بث واستقبال بيانات تقنية المعلومات باستعمال وسائل فنية توفرها تكنولوجيا الإعلام والاتصال. و لكن ما هي الوسائل الفنية التي يمكن للمجرم الإلكتروني استعمالها لاعتراض البيانات؟ هذا ما سنتطرق إليه في الفرع الموالي.

الفرع الثاني: وسائل الاعتراض غير المشروع للبيانات:

فتحت التقنية الرقمية آفاقا واسعة للقيام بالاعتراض دون الحاجة إلى اختراق الدول والمؤسسات بعناصر بشرية تكلف الكثير، بل صار من الممكن الحصول على المعلومات الحساسة والخطيرة عن بعد. في هذا الشأن نصت المادة(07) من (إ.ع.م.ج.ت.م) على أن اعتراض البيانات يتم بكافة الوسائل الفنية التي تمكن المجرم الإلكتروني من اعتراض كافة أشكال النقل الإلكتروني للبيانات مثل: الوسائل التي تتعلق بالتحكم أو مراقبة محتوى الاتصالات، إذ تمكن هذه الأجهزة التي توفرها التكنولوجيا الحديثة في مجال الاتصالات من الحصول على المحتوي بطريقة مباشرة من خلال طريقة الدخول إلى نظام المعالجة الآلية للمعطيات، أو تتم بشكل غير مباشر بواسطة استعمال أجهزة التنصت وتسجيل المعلومات. بل إن مدلول الوسائل الفنية يمكن أن يمتد ليشمل الأجهزة الفنية

---

[1] يقصد بالإنترانت *(INTRANET)*: شبكة إنترنت داخلية تستخدم ذات التقنية لها سرعات مختلفة وكلما بعدت المسافة عن مصدرها قلت سرعتها، فهي شبكة مصغرة بحيث تسمح للأعضاء المسجلين بمنظمة أو مؤسسة أو أي كيان تنظيمي أخر الذي يستخدم البروتوكولات نفسها مثل: *(TCP، IP، HTTP، SMTP، IMAP)* بمزاياها متعددة كسرعة تبادل البيانات، مما أدى إلى انخفاض تكاليف إدارة وإمكانية الوصول إلى المحتوى والخدمات وارتفاع مستوى الحماية الذي لا يمكن مقارنته بمستوى الحماية الموجود على شبكة الإنترنت العادية، راجع شبكة ويكيبيديا على الرابط الآتي:

https://ar.wikipedia.org/wiki/%D8%A5%D9%86%D8%AA%D8%B1%D8%A7%D9%86%D8%AA،تاريخ الاطلاع/2015/12/21 على الساعة:08:10.

المتصلة بخطوط النقل أو الاتصال مثل: أجهزة تجميع وتسجيل الاتصالات اللاّسلكية، إضافة إلى المكونات غير المادية مثل: كلمات المرور والشفرات...إلخ[1].

تعتبر الموجات الكهربائية التي تنتج عن عمل الأنظمة المعلوماتية من أبرز التقنيات المستعملة في اعتراض المعلومات المتنقلة عبر النظام[2]، ومن الوسائل التقنية المستعملة في عملية اعتراض الموجات الكهربائية، الهوائيات *(antennes)*التي يتم ربطها بحاسوب خاص، حيث يمكن عن طريق هذه الهوائيات وعلى مسافة تزيد على ثلاثمائة قدم التقاط الموجات الكهرومغناطيسية[3] المنبعثة من الحاسوب خلال فترة تشغيله مع إمكانية تسجيلها وترجمتها إلى معلومات[4]. وعليه يمكن القول أن اعتراض البيانات أصبح يشمل الجوانب الصناعية والتقنية والتجارية للمؤسسات الاقتصادية. كما يشمل أيضا الجوانب العسكرية والأمنية للدولة بسبب التقدم التكنولوجي الكبير في مجال صناعة الحوسبة والاتصال الذي أسفر عن إيجاد وسائل أكثر فاعلية للاعتراض، والقضايا المطروحة في هذا الشأن كثيرة[5]، فما عادت هذه الوسائل تقتصر على الدول ودوائر المخابرات كما يعتقد معظم الناس بل أصبح بإمكان الأفراد في بعض الدول المتقدمة شراء معدات التجسس وبأسعار معقولة، إما للتجسّس أو لمنعه، وتجدر الإشارة إلى أن هذه الأجهزة ممنوعة من التسويق في الدول العربية ولكن هذا لا يدل على عدم وجودها بل يمكن إدخالها خفية[6].

المطلب الثاني: التزوير المعلوماتي

تتيح تقنية المعلومات مجالا واسعا أمام المجرم الإلكتروني للقيام بأفعال التزوير أو الاحتيال المعلوماتي، والذي يختلف تماما عن مفهومنا لجريمة التزوير التقليدية، سنتناول مفهوم التزوير

---

[1] رشيدة بوكر، المرجع السابق، ص207.

[2] نهلا عبد القادر المومني، المرجع السابق، ص217.

[3] يقصد بالموجات الكهرومغناطيسية: هو ذلك المجال الكهرومغناطيسي المتكون من: مجال كهربي وآخر مغناطيسي ينتشران في الوسط أو الفراغ بسرعة تساوي سرعة الضوء، كما يمكن تمييزها من خلال ثلاث متغيرات أساسية هي: التردّد، الطاقة، والطول الموجي، وتنقسم إلى مصادر طبيعية مثل: الشمس التي تبث تردّدات ما بين 3 إلى300 جيقا هرتز، ومصادر اصطناعية كموجات الراديو والإرسال التلفزيوني والموجات الحرارية ذات الأطوال الموجية القصيرة وخطوط الكهرباء ذات الجهد العالي...إلخ، كما يؤكد العلماء أن تشغيل أي جهاز إلكتروني يتولد عنه مجال كهرومغناطيسي ومنها جهاز الحاسوب، راجع، فؤاد أمين السيد محمد، جرائم الاتصالات وكهرومغناطيسية الموجات،، دراسة تحليلية وتشريعية مقارنة، دار النهضة العربية، القاهرة، مصر، 2014، ص ص42-43.

[4] عفيفي كامل عفيفي، المرجع السابق، ص313.

[5] في هذا المجال، خسرت شركة أمريكية للبترول على مدى أشهر المناقصات التي كانت تدخل فيها، بحيث كانت ترسوا هذه المناقصات على شركة أخرى منافسة لها، بحيث كانت تقدم عروض تقل ببعض الدولات فقط عن عروض الشركة الأولى، وقد اتضح أن ذلك كان نتيجة وجود توصيلات سرية على الحاسوب التابع للشركة الخاسرة للمناقصات بهدف التعرف مسبقا على عروض الأسعار المقدمة، محمد سامي الشوا، المرجع السابق، ص ص213-214.

[6] نهلا عبد القادر المومني، المرجع السابق، ص209.

المعلوماتي في(الفرع الأول) ثم نتطرق إلى مدى خضوع منتوجات الإعلام الآلي لجريمة التزوير في (الفرع الثاني).

الفرع الأول: مفهوم جريمة التزوير المعلوماتي:

تعتبر جريمة التزوير المعلوماتي أو جريمة الاعتداء على منتوجات الإعلام الآلي كأحد أنماط الغش الذي تحل فيه الدعامة المعلوماتية محل السندات في جميع المجالات، الشيء الذي أثار نقاشا حول تحديد مفهوم السند أو المحرر المعلوماتي وتطابقه مع المحرر التقليدي[1]، فالدعامات المادية للحاسب الآلي قد احتلت مكانة المحررات والصكوك، ونظرا لأهمية وخطورة ما تحتويه من بيانات والتي قد تكون محلا للاعتداء بتغيير حقيقتها بقصد الغش في مضمونها، والذي من شأنه إحداث أضرار مادية أو معنوية كتزوير المستخرجات الإلكترونية كالأوراق المالية...إلخ[2]. إن جوهر جريمة التزوير يتمثل في الكذب المكتوب الذي يمس بالثقة العامة في المحررات واستقرارها، حيث يتمثل ركنها المادي في تغيير الحقيقة بإحدى الطرق المحددة قانونا، وأن يكون هذا التغيير في محرر سواء كان رسميا أم عرفيا، وأن يترتب على هذا التغيير ضررا، أما الركن المعنوي فيتمثل في القصد الجنائي العام بالإضافة إلى الخاص[3].

إن جريمة تزوير البيانات تتم بالدخول إلى قاعدة البيانات *(DATABASE)*بطريقة شرعية أو غير شرعية قصد تعديل البيانات سواء بالإلغاء أو بالإضافة[4]، والقضايا كثيرة في هذا المجال نذكر منها حادثة الموظفة بولاية كاليفورنيا الأمريكية التي تقوم بحجز البيانات، أين قامت بتغيير ملكية السيارات المسجلة في الحاسب الآلي [5]. ولتحديد مفهوم جريمة التزوير المعلوماتي، سنتطرق إلى التفرقة بين المستند المعالج آليا والمستند المعلوماتي.

أولا: المستند المعالج آليا: يقصد بالمستند في الاصطلاح القانوني كل دعامة مادية تصلح لأن تدوّن عليها معلومات، ويقصد بالمستند في مجال المعلوماتية كل شيء مادي متميز (قرص

---

1 إدريس النوازلي، جريمة النصب المعلوماتي–قانونا واقعا وقضاء، مطبعة وراقة الوطنية، تونس، ط1، 2015، ص91.

2 آمال قارة، المرجع السابق، ص133.

3 حنان ريحان مبارك المضحكي، المرجع السابق، ص189.

4 منير محمد الجنبيهي وممدوح محمد الجنبيهي، المرجع السابق، ص70.

5 وقعت هذه الحادثة في ولاية كاليفورنيا الأمريكية، حيث عمدت مدخلة البيانات بنادي السيارات وبناء على اتفاقية مسبقة، بتغيير ملكية السيارات المسجلة في الحاسب الآلي، بحث تصبح باسم أحد لصوص السيارات والذي يعمد إلى سرقة السيارة وبيعها. وعندما يتقدم مالك السيارة للإبلاغ يتضح عدم وجود سجلات للسيارة باسمه، وبعد بيع السيارة تقوم تلك الفتاة بإعادة تسجيل السيارة باسم مالكها وكانت تتقاضى مقابل ذلك مبلغ مائة دولار واستمرت في عملها هذا إلى أن قبض عليها. راجع، منير محمد الجنبيهي وممدوح محمد الجنبيهي المرجع السابق، ص70.

مرن، قرص مضغوط، قرص مدمج، أو شريط ممغنط، أو ذاكرة وميضية...إلخ) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام معالجة آلية، ويستوي بعد ذلك أن يكون هذا الشيء قد خرج من الآلة وثم تصنيفه أو تخزينه أو أنه مازال بداخلها انتظارا لاستخراجه[1].

ثانيا: المستند المعلوماتي: ويقصد به تلك المعلومات الخارجة من النظام المعلوماتي كالأوراق المعدة لتسطير المعلومات عليها أو الأقراص المضغوطة أو المدمجة التي لم يسجل عليها أي شيء بعد، والملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة استخدام البرامج، والبطاقات البنكية التي لم تدخل الخدمة بعد ...إلخ[2].

وعليه يمكن تعريف جريمة التزوير المعلوماتي على أنها: "تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية بنية استعمالها"[3].

الفرع الثاني: مدى خضوع منتوجات الإعلام الآلي لجريمة التزوير:

في هذا الصدد نصت المادة (10) من (ا.ع.م.ج.ت.م) على جريمة التزوير وهي:" استخدام وسائل تقنية المعلوماتية من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة" كما نصت المادة (07) من (إ.أ.إ.م) على أن التلاعب في المعطيات الذي ينتج عنه معطيات غير أصلية يعد تزويرا. لكن يشترط أيضا أن يكون محل الجريمة دعامة معلوماتية مخزنة عليها معلومات يمكن تغيير الحقيقة فيها باستخدام الحاسوب، كما لا يلزم أن تكون كل بيانات المحرر مغايرة للحقيقة، وإنما يكفي أن يكون أحد هذه البيانات أو بعضها مكذوبا[4].

تناول المشرع الجزائري جرائم التزوير في المحررات في القسم الثالث والرابع والخامس من الفصل السابع بعنوان: "التزوير" من المادة (214 – 229) من (ق.ع.ج)، والذي يشترط المحرر لوقوع الجريمة[5]، وبالطرق التي نص علها القانون، كما تجدر الإشارة إلى أن المشرع الجزائري ورغم تداركه سد الفراغ التشريعي باستحداث نصوص جديدة في مجال مكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات، إلاّ أنه أغفل تجريم الاعتداءات الواردة على منتوجات الإعلام الآلي، فلم

---

[1] آمال قارة، المرجع السابق، ص ص134-135.

[2] إدريس النوازلي، المرجع السابق، ص91، راجع أيضا، آمال قارة، المرجع السابق، ص135.

[3] حنان ريحان مبارك المضحكي، المرجع السابق، ص212.

[4] هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص325.

[5] لم يعرف المشرع الجزائري المحرّر، حيث نجد له مفهوما في الفقه بأنه: "كل مسطور يتضمن علامات تعطي معنى مترابط ينتقل من شخص لآخر لدى النظر إليها". وفي تعريف آخر بأنه " كتابة مركبة من حروف أو علامات تعبر عن معنى أو فكرة معينة"، راجع هشام محمد فريد رستم، قانون العقوبات، المرجع السابق، ص326.

يستحدث نصا خاصا بالتزوير المعلوماتي، ولم يساير الاتجاه الذي تبنته التشريعات الحديثة التي عمدت إلى توسيع مفهوم المحرّر ليشمل كافة صور التزوير الحديث، مثل: المشرع الفرنسي بموجب نص المادة (9/411) من (ق.ع.ف) حينما نص على تزوير المستندات المعالجة آليا مع استعمالها[1]، فالمشرع الجزائري يستعمل في النصوص التقليدية الخاصة بالتزوير مصطلح "محرر" وهو مصطلح لا يستوعب أفعال التزوير المعلوماتي مما يستدعي تدخلا تشريعيا، إما بتعديل نصوص التزوير التقليدية، أو بإدراج نص خاص بالتزوير المعلوماتي، خاصة بعد تصديق الجزائر على (إ.ع.م.ج.ت.م) التي تنص على جريمة التزوير المعلوماتي بموجب المادة (10) سالفة الذكر.

المطلب الثالث: جريمة الإباحية الإلكترونية والجرائم المرتبطة بها

لم يعد يقتصر انتشار جرائم الإباحية على استعمال الوسائل التقليدية كالجرائد والمجلات الخلاعية والفيديو والقنوات التليفزيونية فقط، وإنما تعد الأمر إلى استعمال الوسائل الحديثة كالحاسوب وشبكة الإنترنت، نظرا لما توفره من السرعة في نشر المواد الإباحية والوصول إلى كافة شرائح المجتمع. سنتطرق إلى مفهوم الإباحية الإلكترونية في(الفرع الأول) ثم نتناول الجرائم المرتبطة بها في (الفرع الثاني).

الفرع الأول: مفهوم الإباحية الإلكترونية:

تعتبر الجريمة الإباحية من أقدم الجرائم المنتشرة عبر كافة المجتمعات، تتسبب في أضرار اجتماعية ونفسية بالغة، لذا نصّت كافة التشريعات على تجريمها قصد حماية الفرد والمجتمع من آثارها المدمرة. إن ما زاد الأمر سوء هو استخدام تقنية المعلومات وشبكة الإنترنت، بحيث سهلت انتشار المواد الإباحية إلكترونيا بعدما كانت تستعمل في الماضي وسائل تقليدية كالمجلات وأشرطة الفيديو، كما تقوم المواقع الإباحية بتسهيل عملية الدخول لمرتاديها قصد الحصول على البرامج والأفلام والصور الإباحية مع إمكانية التحميل المجاني[2]. للأسف انتشرت هذه الجريمة بصورة ملفتة في مجتمعاتنا العربية والاسلامية بما لا يتماشى وقيمها الحضارية، حيث تتجلى آثارها السيئة على ارتفاع جرائم الاغتصاب بصفة عامة واغتصاب الأطفال بصفة خاصة، والعنف الجنسي، وفقدان العائلة لقيمها ومبادئها وتغيّر الشعور نحو النساء إلى الابتذال بدل الاحترام...إلخ[3].

---

[1] *jean Larguier et Autres, Op.Cit,p.241.*

[2] محمد الجنبيهي وممدوح محمد الجنبيهي، المرجع السابق، ص29.

[3] عبد الحليم بوشكيوة، آليات مكافحة الجرائم الماسة بالأخلاق والآداب العامة على الإنترنت، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 01، 2009، ص27.

في هذا الصدد، ذكرت وزارة العدل الأمريكية في دراسة لها أن تجارة الدعارة والإباحية الخلقية تجارة رائجة جدا يبلغ رأس مالها ثمانية (8) مليار دولار ولها أواصر وثيقة تربطها بالجريمة المنظمة. وإن تجارة الدعارة هذه تشمل وسائل عديدة، كالكتب والمجلات وأشرطة الفيديو والقنوات الفضائية الإباحية والإنترنت...إلخ. وتفيد الإحصاءات الاستخبارات الأمريكية *(FBI)* أن تجارة الدعارة هي ثالث أكبر مصدر دخل للجريمة المنظمة بعد المخدرات والقمار حيث إن بأيديهم 85% من أرباح المجلات والأفلام الإباحية[1]. كما تبين الدراسات الحديثة أن دماغ الإنسان الذي ينظر للمحرمات وبخاصة المقاطع الإباحية *(pornographie)* يسلك سوكاً يشبه دماغ ذلك الذي يدمن المخدرات والخمر[2].

بالرجوع إلى (إ.ع.م.ج.ت.م) نصت في المادة (12) منها على الأفعال المكونة لجريمة الإباحية، كما شدّدت العقاب عليها إذا تعلقت بمواد إباحية موجهة لفئة القصر حيث تنص على:"

1-إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.

2- تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر.

3- يشمل التشديد الوارد في الفقرة (2) من هذه المادة حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات."

الفرع الثاني: الجرائم المرتبطة بالإباحية الإلكترونية:

تمثل جريمة الإباحية والجرائم المرتبطة بها خطرا بالغا على فئة الأطفال[3]، حيث تشمل هذه الجرائم تحريض القصر وإغواءهم على أنشطة جنسية غير مشروعة عبر الوسائل الإلكترونية، أو

---

[1] مشعل بن عبد الله القدهي، المواقع الإباحية على شبكة الإنترنت وأثرها على الفرد والمجتمع، بحث منشور على الرابط الآتي: *https://saaid.net/mktarat/abahiah/1.htm*، تاريخ الاطلاع:2015/12/08 على الساعة:08:30.

[2] ففي دراسة حديثة أجريت من قبل باحثين في جامعة كامبردج *(Cambridge University)*، وجدت أن دماغ الإنسان الذي ينظر للمحرمات وبخاصة المقاطع الإباحية *(pornography)*، يسلك سوكاً يشبه دماغ ذلك الذي يدمن المخدرات والخمر. وتعتبر هذه الدراسة الأولى من نوعها بعنوان سنة (2013). حيث استخدم العلماء التصوير بالرنين المغنطيسي لأدمغة مجموعة من الشباب المدمنين على مشاهدة أفلام الجنس، حيث فاجأت نتائج الدراسة العلماء بخطورة المناظر الجنسية، وضرورة الحد من مشاهدتها، يرجى الاطلاع على تفاصيل الدراسة المنشورة على الرابط الآتي:- *http://www.kaheel7.com/ar/index.php/2010-02-02-22-17-58/1577-2013-12-31-03-28-32*، تاريخ الاطلاع:2015/12/08 على الساعة:08:47.

[3] بدأت ظاهرة استغلال الأطفال جنسياً عبر الإنترنت (*Child Pornography on the Internet*) بصورة كبيرة في الغرب خلال السنوات الماضية، مع الاستعمال الواسع لشبكة الإنترنت وانتشار الحواسيب في المدارس والبيوت والمحلات...إلخ، حيث أصدرت الولايات المتحدة أول قانون يقضي بتجريم وحماية الأطفال من المواد الإباحية عام 1978. حيث تقوم مجموعات إجرام منظمة بنشر الصور==

نشر المعلومات عنهم عبر الكمبيوتر والتحرش الجنسي بالقصر عبر الكمبيوتر والوسائل التقنية كاستعمال غرف الدردشة *(Chat room)*، ونشر وتسهيل واستضافة المواد الفاحشة عبر الإنترنت بوجه عام، وتصوير أو إظهار القصر ضمن أنشطة جنسية[(1)]. حيث بلغ عدد المواقع الإباحية سنة 2006 حوالي 4,2 مليون موقع بأرباح مالية قدرت بحوالي 2,5 مليار دولار، كما بينت دراسة أجريت في كل من السويد والنرويج والدنمارك وآيسلاندا وايرلاندا أن نسبة 26% إلى 35 % من الأطفال والمراهقين أعمارهم ما بين 9 و16 سنة قد ارتادوا مواقع إباحية على شبكة الإنترنت[(2)].

وفي الاتجاه نفسه الذي يؤكد على تجريم الإباحية الإلكترونية، أكدت (إ.ع.م.ج.ت.م) في المادة (13) على الجرائم المرتبطة بجريمة الإباحية، حيث نصت على:" المغامرة والاستغلال الجنسي".

بالنسبة للمشرع الجزائري لم ينص على جرائم الإباحية الإلكترونية، رغم انتشارها الواسع باستعمال تقنية المعلومات وخاصة تأثيرها البالغ على فئة القصر الذين تستهدفهم هذه الجرائم بشكل خاص مما يؤثر سلبا على الجانب النفسي لشخصيتهم، وهذا رغم استحداث كل من مصالح الشرطة والدرك الوطني فرقا خاصة للتحقيق في الجريمة الإلكترونية ضد الأطفال، بحيث تعمل هذه الفرق على تقفّي العناوين الإلكترونية للمواقع الإباحية عبر الإنترنت، والتي تحرّض القصّر على العنف والدعارة انطلاقا من معلومات تستمدّها من شكاوى المواطنين.

المطلب الرابع: جرائم تبييض الأموال والمخدرات المرتكبتين عبر الإنترنت:

نتيجة التقدم التقني المذهل في عالم الحوسبة والاتصال، استفاد المجرمون بشكل كبير من هذه التقنية التي تمكنهم بكل سهولة من ارتكاب جرائمهم سواء المتعلقة بتبييض الأموال أو ترويج المخدرات والإفلات في كثير من الأحيان من العقوبة، سنتطرق إلى جريمة تبييض الأموال والأساليب الإلكترونية المستعملة فيها بشيء من التفصل نظرا لخطورتها ضمن هذا الفضاء الإلكتروني، وذلك

==والمقاطع الإباحية للأطفال، واستغلالهم لإقامة حوارات ودردشات جنسية عن طريق الإنترنت، تنطوي على إثارة الشهوات والغرائز الجنسية عن طريق مجموعة من الفتيات القاصرات. لذا أصبحت جرائم استغلال الأطفال قضية عالمية تتطلب ردا فعليا قويا لحمايتهم من التعرض للانتهاكات النفسية والبدنية جرّاء مشاهدتهم للمواد الإباحية، حيث تمثل هذه الممارسات الجانب المظلم من الاستغلال السيئ لشبكة الإنترنت، لأكثر تفاصيل، راجع الموقع الرسمي لوزارة العدل الأمريكية على الرابط الآتي: *https://www.justice.gov/criminal-ceos/child-pornography*، تاريخ الاطلاع:2016/09/0 على الساعة:08:40.

[1] عبد الحليم بوشكيوة، المقال السابق، ص27.

[2] *Myriam Quemener, Réponses pénales face à la cyber pédopornographie, Actualité Juridique Pénal, Editions Dalloz, 2009,p107.*

في (الفرع الأول)، ثم نتناول ما بات يعرف بالمخدرات الرقمية والتي تشكل خطرا مستحدثا لا يقل أهمية عن خطر المخدرات التقليدية وذلك في (الفرع الثاني).

الفرع الأول: جريمة تبييض الأموال والأساليب الإلكترونية المستعملة في ذلك:

إن ظاهرة تبييض الأموال أو غسيل الأموال، ليست ظاهرة وليدة القرن الماضي، بل إنها ظهرت قبل ذلك بكثير ولكن باختلاف الغاية والأسلوب، حيث كان التجار إبان الإمبراطورية الصينية يلجؤون لهذه الظاهرة لإخفاء أموالهم عن طريق استثمارها بمناطق خارج الإمبراطورية خشية مصادرتها من قبل الحكام [1]. كما يقدر بعض الخبراء الدوليين أن هناك ما يتراوح بين 300 إلى 400 مليار دولار من الأموال غير المشروعة يتم تبييضها سنويا، أي ما يعادل 8 % من مجمل التجارة الدولية[2].سنتعرف أولا على جريمة غسيل الأموال طبقا للقواعد التقليدية، ثم نتطرق ثانيا إلى بعض الأساليب الإلكترونية المستعملة في ارتكاب هذه الجريمة .

أولا: جريمة تبييض الأموال طبقا للقواعد التقليدية: نظرا للطبيعة القانونية والاقتصادية المعقدة لهذه الجريمة، حاولت عديد الاتفاقيات والمواثيق الدولية والتشريعات الوطنية وضع تعريف لجريمة تبييض الأموال يشمل كافة أوجه النشاط المجرم.

1- مفهومها: ترجع عمليات تبييض الأموال بوسائلها الفنية الحديثة إلى سنة 1932، حيث بوشرت بشكل منظم بواسطة شخص يدعى (*Meyer Lansky*)، الذي فهم " بأن عولمة أنظمة البنوك وضمان مبدأ السرية المصرفية يسهل من عمليات تبييض الأموال القذرة، وهي تمثل تأثير وسلطة متزايدة"[3]. ونتيجة التطور التكنولوجي الهائل في مجال تقنية المعلومات، ومع تفاقم خطرها على عدة صعد، اهتم المجتمع الدولي بهذه الظاهرة من خلال عقد الاتفاقيات الدولية مثل اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات (اتفاقية فيينا 1988)، والتي ربطت غسيل الأموال بالإتجار غير المشروع في المخدرات. وفي الصدد نفسه، أصدرت لجنة بازل بيانا لسنة 1988 حول منع استخدام النظام المصرفي لأغراض تبييض الأموال، وفي سنة 1989

---

[1] رمزي نجيب القسوس، غسيل الأموال جريمة العصر -دراسة مقارنة، دار وائل للطباعة والنشر، عمان، الأردن، 2002، ص 13، راجع أيضا، مها كامل، عمليات غسيل الأموال، الإطار النظري، مجلة السياسة الدولية، القاهرة، مصر، العدد 146، سنة2001، ص 161.

[2] نادر عبد العزيز شافي، جريمة تبييض الأموال-دراسة مقارنة، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2005، ص201.

[3] *Christophe Emmanuel Lucy, L'odeur de l'argent sale : dans les coulisses de la criminalité financière, Eyrolles société, Paris, 2003, p. 6 .*

أصدرت لجنة العمل المالي الدولية *(GAFI)* توصياتها الأربعين، والتي تعبر عن وجهة نظر الدول الصناعية السبع لمواجهة عمليات غسيل الأموال بالإضافة للعديد من الاتفاقيات الأخرى[1].

كما شملت أيضا بعض الأنشطة المدرة للأموال القذرة (كالإتجار بالأسلحة والاتجار بالنساء والأطفال والاستغلال الجنسي للأطفال، والدعارة، والاتجار في السيارات المسروقة والنقود المزيفة وتجارة المعادن النفيسة...إلخ)[2]. وسواء كانت عمليات تبييض الأموال "ناتجة عن اختلاس أموال أو رشاوى أو تهرب ضريبي، فإن أساليب الأنظمة المالية التي تسمح بإخفاء المصدر الحقيقي للأموال متعددة و كأنها تدور في حلقة غير منتهية" [3].

وعليه يمكن تعريف جريمة تبييض الأموال من خلال المصطلحات الواردة في اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية لسنة 1988 على أنها:" تلك الأموال المتحصل عليها بطريقة مباشرة أو غير مباشرة من ارتكاب جريمة من الجرائم المنصوص عليها في المادة (1/03) ويقصد بها الأصول أيا كان نوعها مادية كانت أم غير مادية [4]. أما المشرع الفرنسي فقد عرّف عملية تبييض الأموال بموجب القانون 96-392 ، الصادر في 13 ماي 1996، المتعلق بمكافحة تبييض الأموال والاتجار في المخدرات والتعاون الدولي في مجال حجز ومصادرة متحصلات الجريمة بأنها:" تسهيل التبرير الكاذب بأي طريقة كانت لمصدر أموال أو دخول لفاعل جناية أو جنحة تحصل منها على فائدة مباشرة أو غير مباشرة"[5].

أما بالنسبة للمشرع الجزائري فلم يعرف جريمة تبييض الأموال في النصوص التشريعية والتنظيمية التي أصدرها في هذا المجال، بحيث استعمل مصطلح" تبييض الأموال" بدلا من مصطلح "غسيل الأموال" متأثرا بالمشرع الفرنسي الذي استعمل نفس المصطلح بالإضافة إلى أنه حدّد الأفعال التي تشكل جريمة تبييض الأموال وآليات مكافحتها، بحيث نص على إنشاء خلية لمعالجة الاستعلام المالي على مستوى وزارة المالية بموجب المرسوم التنفيذي رقم: 02-127 المؤرخ في 07 أفريل 2002 يتضمن إنشاء خلية لمعالجة الاستعلام المالي وتنظيمها وعملها، بالإضافة إلى النص على الأفعال التي تشكل جريمة تبييض الأموال في القسم السادس مكرر من المادة(389 مكرر – المادة 389 مكرر7)، المضاف بموجب القانون رقم: 04-15 مؤرخ في 10 نوفمبر 2004 يتضمن

---

[1] محمد فتحي عيد، الإجرام المعاصر، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، 1999 ، ص280.

[2] محمد عبد الله أبو بكر سلامة، الكيان القانوني لغسل الأموال، المكتب العربي الحديث، الإسكندرية، مصر، 2007، ص26.

[3] *Christophe Emmanuel Lucy, Op.Cit,p.299.*

[4] أنظر: نصوص اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم:95-41 المؤرخ في 28 يناير 1995 (ج.ر) رقم: 7 المؤرخة في: 15 فيفري 1995.

[5] جلال وفاء محمدين ، دور البنوك في عمليات غسيل الأموال، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2004، ص75.

تعديل قانون العقوبات تحت عنوان " تبييض الأموال"[1] ، وعليه تنص المادة (389مكرر) من القانون نفسه على:" يعتبر تبييضا للأموال: تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية... إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها... اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك...".

في السياق نفسه، اعتمد المشرع الجزائري التعريف نفسه بموجب المادة (02) من القانون رقم 05-01 المؤرخ في: 06 فيفري 2005 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما التي نصت على: ... تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية... إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها...[2] . كما نصت أيضا المادة (16) من (إ.ع.م.ج.ت.م) على الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات على: "القيام بعمليات غسل أموال وطلب المساعدة أو نشر طرق القيام بغسل الأموال...".

2- أركان جريمة تبييض الأموال :

أ- **الركن الشرعي:** تنص المادة (389مكرر) من القانون رقم:04-15 على:" يعتبر تبييض للأموال:

- تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية بغرض إخفاء أو تمويه المصادر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته.

- إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، مع علم الفاعل بأنها عائدات إجرامية.

ج- اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها أنها تشكل عائدات إجرامية.

د- المشاركة في ارتكاب أي من الجرائم المقرر وفقا لهذه المادة، أو التواطؤ أو التآمر على ارتكابها ومحاولة ارتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه.

كما نص أيضا على تجريم نفس الأفعال المكونة للجريمة في المادة (02) من القانون رقم 05-01 مؤرخ في 2005/02/06، يتعلق بالوقاية من تبييض الأموال و تمويل الإرهاب ومكافحتهما.

---

[1] المواد من:(389 مكرر - 389 مكرر 7) من القانون رقم:04-15 المعدل والمتمم.

[2] القانون رقم: 05-01 مؤرخ في: 6 فبراير سنة 2005 يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، (ج. ر) رقم:11 المؤرخة في: 09 فبراير 2005، ص ص 04 -05.

ب-الركن المادي: ينحصر السلوك الإجرامي وفق نص المادة (389مكرر) في أربعة صور نتناولها كما يأتي:

✓ **الصورة الأولى:** تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية بغرض إخفاء أو تمويه المصادر غير المشروعة لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته. تتألف هذه الصورة من عنصرين هما: العنصر الأول فعل إيجابي يتمثل في تحويل ممتلكات عائدة من جريمة أو نقلها وتختلف طريقة تحويل المال أو نقله باختلاف طبيعة المال محل الجريمة، فإذا كان المال نقدا يتم تحويله عن طريق صرفه بتحويله إلى عملة أجنبية، أو في شراء شقة ...إلخ ، كما يمكن أن يكون المال في صيغة إلكترونية يتم تحويله إلكترونيا من حساب إلى آخر. أما العنصر الثاني يتمثل في الغرض من تحويل الممتلكات أو نقلها فيستهدف الجاني من وراء ذلك غايتين هما: إما إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات، وإما مساعدة شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعله. وقد يتمثل التحويل في كل تصرف يقع على الأموال أو الممتلكات أو المتحصلات النقدية أو العينية، ومثال ذلك الإيداع ، البيع، الإقراض، المبادلة ...إلخ[1].

✓ **الصورة الثانية:** إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، مع علم الفاعل بأنها عائدات إجرامية، يقصد بالإخفاء حيازة الأموال أو المتحصلات من الجريمة المصدر سواء كانت تلك الحيازة مستترة أم كانت علنية، كما لا يقتصر الإخفاء على معناه المادي فقط، بل يشمل البعض من التصرفات القانونية مثل: استخدام اسم غير حقيقي في شركة وهمية، وقد يكون الإخفاء بالصمت إذا كان هناك التزام بالإعلان عن أمر معين[2]. أما المقصود بالتمويه فهو جملة الأفعال الرامية إلى إخفاء مظهر مشروع على الأموال أو المتحصلات من الجريمة المصدر من خلال مجموعة العمليات المالية المعقدة والمتتابعة لطمس الصفة غير المشروعة للأموال عن طريق استعمال تحويلات داخلية أو خارجية بحيث يتعذر الوصول إلى مصدرها[3].

✓ **الصورة الثالثة:** اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها أنها تشكل عائدات إجرامية. إن المقصود باكتساب الممتلكات هو تلقي الأموال أو

---

[1] عبد العزيز عياد، تبييض الأموال والقوانين والإجراءات المتعلقة بالوقاية منها ومكافحتها في الجزائر، دار الخلدونية ، الجزائر،2007 ص ص 41-42.

[2] سامية دلندة، ظاهرة تبييض الأموال، مكافحتها والوقاية منها، نشرة القضاة، العدد 60، الجزائر، (ب. س. ط)، ص247 .

[3] المرجع نفسه، ص 248.

المتحصلات على سبيل التكسّب أو الترويج كما أن لفظ الاكتساب هنا عام ، فلا يشترط أن يكون الحصول على المال من الجريمة المصدر بطريق مباشر، بل يمكن الحصول عليها بطريق غير مباشر مثل الأرباح الناتجة من الأموال المتحصلة من الجريمة المصدر ، أما الحيازة فهي الاستئثار بالشيء على سبيل الملك دون الحاجة للاستيلاء عليه، فيكفي لاعتبار الشخص حائزا و لو لم تكن له السيطرة المادية مثل إجراء قروض وهمية[1].

✓ **الصورة الرابعة:** المشاركة في ارتكاب أي من الجرائم المقرر وفقا لهذه المادة، أو التواطؤ أو التآمر على ارتكابها ومحاولة ارتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه يعد تبييضا للأموال، وأن كل فعل من هذه الأفعال يصلح أن يشكل صورة من صور هذه الجريمة.

كما تتفق جل التشريعات المجرمة لظاهرة تبييض الأموال، أن هذه الجريمة تابعة تتطلب لاكتمال بنيانها القانوني وقوع جريمة أولية أو أصلية هي مصدر الأموال غير المشروعة، وهي العنصر المفترض لجريمة تبييض الأموال، وعلى ضوء ذلك فإن الجريمة الأولية هي:" كل نشاط إجرامي فعل أو امتناع عن فعل تحصلت منه بطريقة مباشرة أو غير مباشرة أموالا غير مشروعة تعتبر محلا لجريمة غسيل الأموال، هذه الجريمة السابقة هي المصدر لجريمة التبييض"[2].

ج-الركن المعنوي: جريمة تبييض الأموال جريمة عمديه ويلزم لوقوعها توفر القصد الجنائي العام والقصد الجنائي الخاص، فبالنسبة للقصد الجنائي العام الذي يقوم على عنصري العلم والإرادة فيجب أن يعلم الجاني أن المال محل التبييض متحصل من عمل إجرامي، فإذا كان الجاني يجهل ذلك فلا يتوفر القصد الجنائي العام لديه لتخلف أحد عناصره وهو العلم وبالتالي لا تقوم الجريمة، كما يجب أن يكون العلم معاصرا للنشاط الإجرامي. فضلا عن اتجاه ارادة الجاني للقيام بالنشاط الجرمي المكون لهذه الجريمة. أما بخصوص القصد الجنائي الخاص المنصوص عليه في الفقرة الأولى من المادة (389مكرر)، يتوافر إذا كان الجاني يقصد من نشاطه إما إخفاء أو تمويه المصادر غير المشروعة لتلك الممتلكات، أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته [3].

د-العقوبات المقررة: نصت المادة(389 مكرر1) على أنه: "يعاقب كل من قام بتبييض الأموال بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 1.000.000 دج إلى 3.000.000 دج".

---

[1] المرجع نفسه، ص 250.

[2] عبد الفتاح بيومي حجازي، جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، دار الفكر الجامعي، الإسكندرية مصر،2005، ص124.

[3] سامية دلندة ، المرجع السابق، ص ص 257-258.

هـ- الظروف المشددة: نصت المادة(389 مكرر2) على أنه:" يعاقب كل من ارتكب جريمة تبييض الأموال على سبيل الاعتياد أو باستعمال التسهيلات التي يمنحها نشاط مهني أو في إطار جماعة إجرامية، بالحبس من عشر (10) سنوات إلى خمس عشر (15) سنة وبغرامة من 4.000.000 إلى 8.000.000 دج".

✓ **المصادرة** : طبقا للمادة(389 مكرر4) من قانون العقوبات حيث تنص:" تحكم الجهة القضائية المختصة بمصادرة الأملاك موضوع الجريمة المنصوص عليها في هذا القسم، بما في ذلك العائدات والفوائد الأخرى الناتجة عن ذلك في أي يد كانت ، إلا إذا أثبت مالكها أنه يحوزها بموجب سند شرعي وأنه لم يكن يعلم بمصدرها غير المشروع..."

و-العقوبات التكميلية: تنص المادتان(389 مكرر5 و389 مكرر6) على تطبيق عقوبة واحدة أو أكثر من العقوبات التكميلية على الشخص الطبيعي ، وأيضا عقوبة المنع من الإقامة على الإقليم الوطني بصفة نهائية أو لمدة عشر سنوات على الأكثر، على كل أجنبي مدان بإحدى الجرائم المنصوص عليها في المادتين(389 مكرر1 - 389 مكرر2) [1].

ثانيا: بعض الأساليب الإلكترونية المستعملة في عمليات تبييض الأموال: إن الأساليب المستخدمة في عمليات التبييض كثيرة ومتنوعة"، ففي هذا الشأن يقول الدكتور أوليفي جيراز *(Olivier Jerez)*" لا يمكن تعيين قائمة بطرق وأساليب تبييض الأموال"[2]، فمرتكبو هذه الجرائم يلجؤون لأساليب عديدة طبقا لظروف كل عملية، وطبقا للمبالغ المالية الموجودة وأيضا للمكان الذي تتم فيه عملية التبييض. تعتبر المصارف والبنوك أكثر المؤسسات التي تتم من خلالها عمليات تبييض الأموال فهي الوجهة المفضلة لأصحاب الأموال القذرة لتنظيف عائداتهم دون التعرض لمخاطر كشفهم، وذلك بسبب ما توفره التقنية الحديثة من وسائل سريعة يصعب معها ملاحقة هذا النوع من الجرائم، سنتطرق إلى أهم الوسائل:

1- بطاقات الائتمان: يلجأ أصحاب الدخول غير المشروعة إلى استعمال أحدث الوسائل التكنولوجية قصد إزالة صفة عدم المشروعية على أموالهم وإلباسها صفة المشروعية، وهذا عبر إجراءات مصرفية مختصة تمتاز في بعض الأحيان بالتعقيد الذي يصعب معه اكتشاف أصل تلك الأموال ومصدرها[3]، ولقد أصبح قطاع البنوك كأي قطاع تجاري يتداول الأموال من خلال الوسائل التكنولوجية الحديثة كاستخدام البطاقات الممغنطة والتليفون أو بواسطة شبكة الإنترنت دون الحاجة

---

[1] المادتان(389 مكرر5 - 389 مكرر6) من القانون رقم: 04-15المعدل والمتمم.

[2] *Olivier Jerez, Le blanchiment de l'argent, BANQUE Edition, France, 2ème édition, 2003, p.71.*

[3] محمد عبدالله الرشدان، جرائم غسيل الأموال، دار قنديل للنشر والتوزيع ،الأردن، 2007، ص102.

إلى المرور عبر البنوك توفيرا للجهد وتحسينا للخدمة.[1]. تأكيدا لذاك يشير التقرير الذي أعدته الأمم المتحدة وصندوق النقد الدولي إلى أن 28,5 مليار دولار من الأموال القذرة تنقل سنويا عبر الإنترنت لتخترق حدود 67 دولة لغسلها[2].

2- التحويل الإلكتروني للنقود: هناك صعوبة كبيرة في تعقب الأموال القذرة إذا تم تحويلها بالطريق الإلكتروني أو الطريق البرقي، ويتم ذلك حينما يقوم مبيضو الأموال بإيداع أموالهم القذرة في البنوك بطريقة آمنة، ثم يقومون بعد ذلك بتحويلها برقيا إلى حسابات شركات وهمية خارج الدولة في بلدان تتسم بقوانين مطلقة في مجال السرية المصرفية، بحيث يصبحون في مأمن من ملاحقات الأجهزة المختصة بمكافحة تبييض الأموال[3].وفقا لنظام سويفت *(Swift)*، فإن البنك الذي يقوم بتنفيذ التحويل لا يعلم الغرض من عملية التحويل ذاتها، ذلك أن البنك هو وحده الذي يقع عليه واجب التحري عن غرض العميل من هذا الاستخدام، وعليه فإن التحويلات الصادرة من بنوك أجنبية غالبا ما تكون خالية من إسم العميل المنشئ، إذ تقتصر على ذكر عبارة " إن عميلنا يرغب في تحويل ... إلى عميلكم..."[4].

3- أجهزة الصرف الآلي: تستخدم أجهزة الصرف الآلي *(ATM)* في عمليات إيداع أو سحب الأموال القذرة من الحسابات المصرفية، وهذا بهدف التخلص من الإجراءات المتعلقة بتعبئة النماذج الخاصة بعمليات الإيداع والصرف، التي تعد أدلة إثبات يمكن الرجوع إليها في حالة الشك في مصدر الأموال المودعة، كما تستعمل أجهزة الصرف الآلي في عمليات غسل الأموال، وذلك عن طريق إجراء العديد من عمليات الإيداع والسحب للأموال المراد غسلها في يوم واحد، ومن عدة أماكن دون أن تلفت نظر السلطات المختصة لاكتشافها[5].

4- بنوك الإنترنت: تعد هذه الوسيلة أهم وأخطر الوسائل التكنولوجية الحديثة لعمليات تبييض الأموال، نظرا للتقدم الهائل في مجال تكنولوجيا المعلومات ووسائل الاتصال وانتشار الإنترنت على نطاق واسع وسهولة الحصول على خدماتها. إن انتشار ظاهرة البنك المحمول وبرغم حداثتها، إلا أنها تثبت أن البنك يحقق أرباحا تعادل ستة أضعاف ما يحققه البنك العادي في تعاملاته التقليدية لأنه يستخدم التكنولوجيا لتحسين علاقاته وتوسيع تعاملاته عن طريق استعمال البيانات الشخصية

---

[1] *Olivier Jerez, Op.Cit,p.132.*

[2] حسين محمدي بوادي، إرهاب الإنترنت الخطر القادم، دار الفكر الجامعي، الإسكندرية، مصر، ط1، 2008، ص63.

[3] عبد الفتاح بيومي حجازي، جريمة غسل الأموال، المرجع السابق، ص 64.

[4] المرجع نفسه، ص65 .

[5] علي لعشب، الإطار القانوني لمكافحة غسل الأموال، ديوان المطبوعات الجامعية، الجزائر، 2007، ص36.

بطريقة ذكية لكي يقوم بتسويق خدمات من نوع جديد للعملاء[1].إن نظام البنوك عبر الإنترنت *(Cyberbanque)* ليست في الواقع بنوكا بالمعنى الفني الشائع والمألوف، إذ لا تقوم بقبول الودائع أو تقديم التسهيلات المصرفية أو غيرها من العمليات المصرفية المعتادة، ولكنها عبارة عن وسيط في القيام ببعض العمليات المالية وعمليات البيوع، فيقوم المتعامل بإدخال الشفرة السرية في الكمبيوتر ومن ثمة يستطيع تحويل الأموال[2].

5- الهاتف الخلوي: يعتبر الهاتف الخلوي، أو الهاتف المحمول *(mobile)* عنصرا جديدا أضافته التكنولوجيا إلى قائمة تقنيات تبييض الأموال، إذ يسمح الهاتف الخلوي للمنظمات الإجرامية ولكبار المجرمين، بإجراء مخابرات سريعة جدا مع إخفاء هوية المتصل، وتتمتع منظمات تهريب الأموال المتطورة بميزة استعمال وقراءة إشارات البث التي تصدرها الهواتف الخلوية، وكشف أرقام الهواتف المتسلسلة التي تعرف بالأرقام المتسلسلة الإلكترونية *(Electronic Série number)* فيمكنهم القيام بكافة أعمالهم الإجرامية في كافة الأماكن الخاصة والعامة، ولهذا فإن مراقبة هذه الهواتف بالإضافة إلى مراقبة الهواتف العادية، تعتبر السبيل الوحيد في بعض الأحيان لاكتشاف العديد من الجرائم لاسيما جريمة تبييض الأموال، لأن مبيضي الأموال يقومون بتخطي ملاحقتهم بتغيير أرقام هواتفهم وأجهزة إنذارهم باستمرار قصد تضليل المحققين وبالتالي الإفلات من قبضة العدالة[3].

لقد تناول المشرع الجزائري تعريف الأموال التي تقع عليها جريمة تبييض الأموال، ولم يفرق بين الأموال المادية والمعنوية وكذا الأموال المنقولة وغير المنقولة، كما لم يحدد وسيلة معينة للحصول على تلك الأموال، ومنها الصكوك والوثائق بما فيها الشكل الإلكتروني أو الرقمي وفقا لنص المادة (1/04) من القانون رقم:05-01 سالف الذكر[4]مسايرا في ذلك المشرع الفرنسي، فجميع العمليات التي يتم بها تبييض الأموال يمكن أن تدخل في الجريمة بصورتها المعلوماتية، فالجريمة المرتكبة بواسطة شبكة الإنترنت لا تختلف عن الجريمة المرتكبة بالوسائل التقليدية سوى في استخدام

---

[1] عبد الفتاح بيومي حجازي، جريمة غسل الأموال، المرجع السابق، ص73.

[2] جلال وفاء محمدين، المرجع السابق، ص ص34 -35.

[3] نادر عبد العزيز شافي، المرجع السابق، ص ص 329-330.

[4] تنص المادة (1/04) من القانون رقم:05-01 على:" يقصد في مفهوم هذا القانون ما يأتي: الأموال: أي نوع من الأموال المادية أو غير المادية، لاسيما المنقولة أو غير المنقولة التي يحصل عليها بأية وسيلة كانت، والوثائق أو الصكوك القانونية أيا كان شكلها بما في ذلك الشكل الإلكتروني أو الرقمي...".

الوسيلة[1]، وهذا مسلك محمود من المشرع الجزائري في سياسته الجنائية المتعلقة بمكافحة الجرائم المستحدثة التي تستعمل التقنية المعلوماتية وسيلة لارتكابها.

الفرع الثاني: جرائم المخدرات المرتكبة عبر الإنترنت:

أدت الثورة الرقمية إلى انتشار شبكات المعلومات وأهمها شبكة الإنترنت التي يمكن من خلالها تداول المعلومات ونقلها بسهولة ويسر لجميع أنحاء العالم مما ساهم في الاستفادة المثلى من ثورة المعلومات، لكن بالمقابل تعد المشاركة غير المشروعة بين الاتجار في المخدرات والمؤثرات العقلية بكافة أصنافها[2]واستغلال شبكة الإنترنت مشكلة كبيرة ضاعفت من ارتكاب جرائم المخدرات قياسا باستعمال الطرق التقليدية، كما تستطيع شبكة الإنترنت توفير فضاء ملائم لمنظمات الاتجار بالمخدرات مما يمكنها من تحقيق أرباح إضافية وانتشار أوسع لأنشطتهم. حيث بات من الأسهل جدا بيع وشراء المخدرات عبر الإنترنت حيث لا يوجد وسيط بين البائع والمشتري إضافة إلى الخدمات التي تقدمها بعض المواقع الإلكترونية حول كيفية زراعة وصناعة المخدرات على اختلاف أصنافها[3].

في هذا الصدد، تتعدد الجنح المتعلقة بالمخدرات كالاستهلاك أو الحيازة أو التسليم أو العرض بهدف الاستعمال الشخصي...إلخ، سنتطرق أولا وبإيجاز إلى أركان جرائم المخدرات والمؤثرات العقلية

---

1 فايز محمد راجح غلاب، الأطروحة السابقة، ص50.

2 أوضح تقرير مكتب الأمم المتحدة الخاص بالمخدرات والجريمة *(UNODC)* لسنة 2014 أن تناول المخدرات يحدث خسائر كبيرة في الأرواح، حيث يبلغ معدل الوفاة 40 شخصا لكل مليون من السكان الذين هم في سن من 15 إلى 64 سنة وعلى الصعيد العالمي، يقدر أنه في عام 2012 كان ما بين 261 مليون شخص و423 مليون شخص أي: ما نسبته من 5.3%إلى07% من سكان العالم في سن51-46 عاما، قد تناولوا مرة واحدة على الأقل مادة تنتمي إلى فئة القنب أو الأفيون أو الكوكايين...إلخ، لأكثر تفاصيل، يرجى الاطلاع على هذا التقرير المنشور على الموقع الرسمي لمكتب الأمم المتحدة على الرابط الآتي: *http://www.unodc.org/wdr2014/* ، تاريخ الاطلاع:2016/02/01 على الساعة:15:32 .

3 حيث يشير تقرير صادر عن الإنتربول إلى أن 890 مليون متعاطي للمخدرات معظمهم في آسيا وأروبا وأمريكا الشمالية يستخدمون شبكة الإنترنت بإمكانياتها المتاحة في الحصول على المخدرات، حيث برزت مشكلة شديدة الخطورة تمثلت في إدخال المخدرات والمؤثرات العقلية نطاق العالم الافتراضي، وظهر مصطلح جديد وهو(*Cyber Drugs*). في هذا الشأن أشارت لجنة البلدان الأمريكية لمكافحة تعاطي المخدرات التابعة لمنظمة الدول الأمريكية في تقريرها لسنتي 1999و2000، أن نصف سكان الكرة الأرضية يستخدمون شبكة الإنترنت في زيادة إنتاج المخدرات المصنعة واتساع رقعتها. وفي شهر فبراير من سنة 2000 صدر قرار الجمعية العامة للأمم المتحدة رقم 132/404 مشيرا إلى أهمية التعاون الدولي في مكافحة مشكلة المخدرات العالمية، حيث جاء في ديباجة القرار "وإذ تسلم الجمعية بأن استخدام شبكة الإنترنت يتيح فرصا جديدة وتفرض تحديات جديدة بالنسبة للتعاون الدولي في مكافحة إساءة استعمال المخدرات وإنتاجها والاتجار بها على نحو غير مشروع، وإذ تسلم بالحاجة إلى زيادة التعاون بين الدول وتبادل المعلومات بما في ذلك ما يتصل بالخبرات الوطنية بشأن إساءة استعمال المخدرات والاتجار غير المشروع بها بواسطة استخدام شبكة الإنترنت..."، حسين بن سعيد الغافري الإنترنت وآفة المخدرات، ورقة بحثية مقدمة لمؤتمر أمن المعلومات والخصوصية في ظل قانون الإنترنت القاهرة 2-4 يونيو2008 منشور على الرابط الآتي:*http://www.shaimaaatalla.com/vb/showthread.php?t=3939* ، *تاريخ الاطلاع:2016/02/01* على الساعة:14:53.

والعقوبات المقررة لها وفق القواعد التقليدية، وكذا دور الإنترنت في ارتكاب هذه الجرائم، وهذا قصد معرفة تناسب نصوص القانون الجزائري مع خصوصية هذه الجريمة التي ترتكب عبر الإنترنت ، ثم نتعرف ثانيا على ما بات يعرف بالمخدرات الرقمية التي ترتكب عبر شبكة الإنترنت.

أولا: جرائم المخدرات وفقا للقواعد التقليدية: تقوم هذه الجريمة على الأركان الآتية:

1-الركن الشرعي: جاء القانون رقم:04-18 المؤرخ في:2004/12/25 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بهما لتدارك الفراغ الذي كان موجودا في هذا المجال من جهة، وتجاوبا مع الالتزامات المرتبة عن الاتفاقيات الدولية التي صادقت عليها الجزائر من جهة أخرى، حيث عرفت المادة (02) من هذا القانون المقصود بالمخدرات والمؤثرات العقلية بكافة اصنافها[1]. حيث جرّم المشرع الجزائري عدة أنشطة متعلقة بالمخدرات والمؤثرات العقلية يمكن حصرها في ثمانية (08) صور، أربع منها جنايات وأربع جنحا، إضافة إلى صورتين خاصتين[2] وهذا بموجب المادة (12) إلى غاية المادة (22) من القانون سالف الذكر.

2- الركن المادي: يتألف من عدة صور:

أ- بالنسبة للجنح: يتكون ركنها المادي من:

- الاستهلاك أو الحيازة من أجل الاستهلاك الشخصي: الفعل المعاقب عليه بنص المادة(12).
- التسليم أو العرض للغير بهدف الاستعمال الشخصي: الفعل المعاقب عليه بنص المادة(13).
- تسهيل للغير الاستعمال: الفعل المعاقب عليه بنص المادتين: (16-15)
- إنتاج المواد المخدرة أو المؤثرات العقلية بطريقة غير شرعية: الفعل المعاقب عليه بنص المادة(17).

ب- بالنسبة الجنايات: يتكون ركنها المادي من:

✓ تسيير أو تنظيم أو تمويل إنتاج المواد المخدرة أو المؤثرات العقلية: الفعل المعاقب عليه بنص المادة(18).

✓ تصدير أو استيراد مخدرات أو مؤثرات عقلية بطريقة غير مشروعة: الفعل المعاقب عليه بنص المادة(19).

---

[1] تنص المادة (02) من القانون رقم:04-18 المؤرخ في:2004/12/25 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بهما على: "يقصد في مفهوم هذا القانون ما يأتي: المخدر: "كل مادة طبيعية كانت أم اصطناعية من المواد الواردة في الجدولين الأول والثاني من الاتفاقية الوحيدة للمخدرات لسنة1961...المؤثرات العقلية: كل مادة طبيعية كانت أم اصطناعية أو كل منتوج طبيعي مدرج في الجدول الأول أو الثاني أو الثالث أو الرابع من اتفاقية المؤثرات العقلية لسنة 1971..." (ج.ر) رقم:83 المؤرخة في:2004/12/26، ص ص03-08 .

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، المرجع السابق، ص ص462-468.

✓ زرع بطريقة غير مشروعة خشخاش الأفيون وشجيرة الكوكا أو نبات القنب: الفعل المعاقب عليه بنص المادة(20) .

✓ صناعة أو نقل أو توزيع سلائف أو تجهيزات بهدف استعمالها: الفعل المعاقب عليه بنص المادة(21).

3- الركن المعنوي: يقوم الركن المعنوي لجرائم المخدرات على القصد الجنائي العام بعنصريه العلم والإرادة، إضافة إلى القصد الجنائي الخاص في جرائم الاتجار في المخدرات والمؤثرات العقلية. فإذا علم المتهم بأنه يقوم بفعل من الأفعال التي تقوم عليها جرائم بالمخدرات أو المؤثرات العقلية سواء بحيازتها أو استهلاكها أو تقديمها للتعاطي...إلخ، واتجهت إرادته الحرة المدركة لطبيعة هذه الأفعال إلى ارتكابها، وجب ردعه بتوقيع العقوبة عليه. كما يجب أن يتوفر إلى جانب القصد الجنائي العام القصد الجنائي الخاص في جرائم الاتجار بالمخدرات بأن يكون ذلك بنية الاتجار فيها، كما يتطلب أيضا القصد الجنائي الخاص في جريمة الحيازة للمخدرات بنية التعاطي أو الاستعمال الشخصي[1].

4- العقوبات المقررة: نصت المواد من:(12 - 29) من القانون نفسه على العقوبات الأصلية بالنسبة: الفاعل الأصلي- الاستهلاك- العود- الشروع- التحريض- السجن المؤبد- الشخص المعنوي، إضافة إلى العقوبات التكميلية[2].

ثانيا: دور الإنترنت في جرائم المخدرات والمؤثرات العقلية: نظرا للخدمات الواسعة التي تقدمها شبكة الإنترنت، يمكن تلخيص دورها في الترويج والمتاجرة بالمخدرات والمؤثرات العقلية فيما يأتي:

أ-إعطاء صورة زائفة عن المخدرات: يوجد على شبكة الإنترنت طوفان هائل من المواقع الإلكترونية التي تحوي على صور ومعلومات زائفة للمخدرات التي تنقل متعاطيها إلى جنة الأحلام فالمروّج بات في استطاعته استخدام صفحات الإنترنت لتقديم شرح مفصل عن المخدرات والمؤثرات العقلية من حيث أنواعها وأساليب معالجتها وكيفية تعاطيها، بل وصل الأمر إلى أن بعض المواقع تقدم وصفات لصناعة المخدرات منزليا بوسائل بسيطة، وبمواد أولية تباع قانونيا في كل بلدان العالم وفي هذا السياق يقول السيد: كيلي فوستر *(Kelly Foster)*الناطق باسم تحالف *(Community Anti-Drug Coalitions of America)* المناهض للمخدرات "أن تحالفه خسر معركته الأولي في ساحات الإنترنت أمام العديد من المواقع التي تروج ثقافة المخدرات"، ولعل أخطر ما في الموضوع أن ثمة علاقة وطيدة بين ثالوث المراهقة والمخدرات والإنترنت فضلا عن الدعاية التي تحفل بها هذه

---

[1] فايز محمد راجح غلاب، الأطروحة السابقة، ص58.

[2] أنظر: المواد من: (12 - 29) من القانون رقم:04-18 المؤرخ في:2004/12/25 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بهما.

المواقع والمعلومات المضللة عن المخدرات وكيفية الوصول إلى موزعيها[1].

من جانب آخر، أكد تقرير الهيئة الدولية لمراقبة المخدرات لعام 2012 وجود دليل واضح على استعمال شبكة الإنترنت كوسيلة لتوزيع المواد ذات التأثير النفساني، كما تحض الحكومات على رصد أنشطة المواقع الشبكية التي تبيع هذه المواد[2]. وفي تقرير نشرته شبكة *(CNN)* الإخبارية الأمريكية على موقعها الإلكتروني، ذكرت فيه قيام السلطات الاتحادية والمحلية في عدد كبير من الولايات الأمريكية بحملة واسعة بهدف تعقب مروجي المخدرات الذين يوزعون العقار المخدر المسمي *(GHB)* عبر شبكة الإنترنت، حيث ألقت القبض على العشرات منهم في مختلف المدن الأمريكية[3].

ب-الاتجار بالمخدرات والمؤثرات العقلية: لم يقتصر الأمر على استخدام الإنترنت على عمليتي البيع والعرض للمخدرات والمؤثرات العقلية، وإنما امتد ليشمل بيع التقنية ذاتها كوسيلة للإتجار المذكور، ومن الأمثلة على بيع التقنية: بيع موقع إلكتروني مشهور بكثرة الولوج إليه والشراء من خلاله، أو التنازل عن بريد إلكتروني يتم من خلاله الطلب، أو الاشتراك في إحدى غرف المناقشة التي يتم من خلالها التعامل غير المشروع بالمخدرات والمؤثرات العقلية مقابل الالتزام بدفع مبلغ مالي أو القيام بإعداد تقنية خاصة لمحركات البحث (*Search Engine)* مهمتها المساعدة في الانتقال إلى المواقع الخاصة بأنواع معينة من المخدرات أو استخدام تقنية خاصة يتم توزيعها على العملاء والتجار عبر شبكة الإنترنت[4].

ج-المطالبة بإباحة تعاطي المخدرات :تساعد شبكة الإنترنت إلى حد كبير المطالبين بإخراج تعاطي المخدرات من دائرة التجريم، مستندين في ذلك إلى أن الكثير من التشريعات سيما الغربية لا تجرم الانتحار أو إصابة الشخص نفسه. ولقد وجد أنصار هذا الاتجاه ضالتهم في شبكة الإنترنت بخدماتها الكثيرة، ويأتي في مقدمة المطالبين بإباحة المخدرات مجموعة *(Drug Reform Coordination Network)* ويتزعمها ديفيد بوردين *(David Borden)*، والتي تعمل عبر شبكة الإنترنت منذ عام 1993 . كما يطلق على مواقع الإنترنت التي تطالب بإباحة تعاطي المخدرات إسم مواقع الثقافة المضادة (*Counter Culture*) ، ومن أشهرها موقع(*www.paranoia.com)* والذي

---

[1] يوسف حسن يوسف، المرجع السابق، ص122.

[2] تقرير الهيئة الدولية لمراقبة المخدرات لسنة 2012، متاح على موقع الهيئة الرسمي على الرابط الآتي:
http://www.ginad.org/ar/info/researches/2826/International-Narcotics-Control-Strategy-Report-March-2012 ، تاريخ الاطلاع:2016/02/06 على الساعة:09:25، ص51.

[3] منير محمد الجنبيهي وممدوح محمد الجنبيهي، المرجع السابق، ص77 وما بعدها.

[4] حسين بن سعيد الغافري، الإنترنت وآفة المخدرات، المداخلة السابقة، ص 15 وما بعدها.

مُنع مؤخرا من قبل السلطات الأمريكية لقيامه بحملات تندد بتجريم تعاطي المخدرات وتنعت مصدري هذه القوانين بألفاظ لا تليق[1].

تناولنا صور السلوك الإجرامي في جرائم المخدرات والمؤثرات العقلية وفقا للقواعد التقليدية وبالرغم من نجاح المشرع الجزائري في مكافحة هذا النوع الخطير من الجرائم الذي يفتك بشرائح واسعة من المجتمع، ومع انتشار الاتجار في المخدرات والمؤثرات العقلية باستعمال شبكة الإنترنت، إلا أن القانون رقم:04-18 لم يتضمن نصا صريحا لتجريم هذه الأفعال حينما ترتكب بواسطة شبكة الإنترنت مثلما فعل العديد من المشرعين كالمشرع الفرنسي والسعودي والإماراتي[2].

وعليه يختلف الأمر بالنسبة للركن المادي حينما ترتكب بواسطة شبكة الإنترنت، فهو يقوم على:

– الترويج والاتجار بالمخدرات والمؤثرات العقلية على شبكة الإنترنت عن طريق عرض المواد المخدرة والمؤثرات العقلية في مواقع معينة والتواصل مع العملاء من مختلف الدول والاتفاق على عملية الشراء والنقل واستلام الأموال، مما ساعد على نقل رؤوس الأموال بسرعة كبيرة على مستوى العالم[3] .

– إعداد مواقع متخصصة على شبكة الانترنت تتولى عرض الوصفات الطبية للبيع التي تحتوي على أدوية مخدرة، وتوضيح كيفية صنع المخدرات عن طريق الوصفات الشعبية بالاستعانة بمواد غذائية تباع في الأسواق وبمستحضرات متوفرة على مستوى الصيدليات والمستشفيات، حيث تقوم هذه المواقع بترويج المخدرات للمحافظة على سوق الطلب وزيادة أرباحهم[4].

ثالثا: المخدرات الرقمية وشبكة الإنترنت: لم يقف الأمر عند الترويج والاتجار بالمخدرات والمؤثرات العقلية باستعمال شبكة الإنترنت، كما لم يعد استهلاك المخدرات مقصوراً على حقنها في الوريد أو بمضغها أو شمها أو تدخينها، وإنما تطور الفكر الإنساني ليحول نظم التعاطي التقليدية إلى نظام تعاطي إلكتروني أو رقمي يحدث التأثير نفسه الذى تحدثه المخدرات الطبيعية أو الصناعية الأخرى وربما أشدّ من ذلك. فلقد أُستحدث نوع جديد من المخدرات يسمي بالمخدرات الرقمية ***(cyber***

---

[1] المداخلة نفسها، ص15.

[2] تنص المادة (4/06) من نظام مكافحة الجرائم المعلوماتية السعودي الصادر في:2007/03/26 على:" يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ﷼ أو بإحدى هاتين العقوبتين: كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية...إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للإتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها أو طرق تعاطيها، أو تسهيل التعامل بها..."

[3] فايز محمد راجح غلاب، الأطروحة السابقة، ص56.

[4] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، القاهرة، مصر 2004، ص661.

(drugs) يستعمل شبكة الإنترنت كوسيلة للترويج لها والاتجار فيها، وهي أكثر خطورة من المخدرات التقليدية لما لها من تأثير مدمر على دماغ الانسان قد يؤدي به إلى الوفاة مباشرة بعد استهلاكها، لكن بالمقابل ما هو مفهومها؟ وكيف تعمل؟.

1- مفهومها: المخدرات الرقمية أو ما يُطلق عليه اسم :*(Digital Drugs)* هي عبارة عن مقاطع نغمات يتم سماعها عبر سماعات بكل من الأذنين، بحيث يتم بث ترددات معينة في الأذن اليمني على سبيل المثال وترددات أقل إلى الأذن اليسرى[1]، تعتمد على جرعات موسيقية صاخبة توحي بنشوة التعاطي بين الشباب.. وتعطيهم إحساسا بالسعادة غير الدائمة التي قد تؤدي إلى وفاة المستمع..أو هي:" نوع من أنواع الموسيقي الصاخبة تحدث تأثيرًا على الحالة المزاجية يحاكي تأثير الماريجوانا والحشيش والكوكايين، يتم الاستماع إليها من خلال سماعات الأذن أو مكبرات الصوت ويقوم الدماغ بدمج الإشارتين، ما ينتج عنه الإحساس بصوت ثالث يدعى *(binaural beat)* وتؤدي إلى خلق أوهام لدى الشخص المستمع وتنقله إلى اللاّوعي، وتهدده بفقدان التوازن النفسي والجسدي[2].

2- خطرها: يتم الترويج إلى المخدرات الرقمية، من خلال ملفات صوتيه في شكل*(mp3)* يتم تحميلها من مواقع إلكترونية بمقابل مادي من أجل الإدمان النفسي، وتلحق المخدرات الرقمية لمتعاطيها الضرر نفسه الذي تسببه المخدرات التقليدية. فهي تؤثر على ردة فعل الدماغ بخلق حالة

---

[1] في عام 1839 اكتشف العالم الفيزيائي *(Heinrich Wilhelm Dove)*أنه إذا سلطت ترددين مختلفين قليلاً عن بعضهما لكل إذن فإن المستمع سيدرك صوت نبض سريع. سميت هذه الظاهرة بـ *(binaural beats)*استخدمت هذه الآلية لأول مرة عام 1970 من أجل علاج بعض المرضى النفسيين لاسيما الاكتئاب الخفيف والقلق، وذلك عند رفضهم العلاج الدوائي حيث كان يتم تعريض الدماغ إلى تذبذبات كهرومغناطيسية تؤدي لفرز مواد منشطة كالدوبامين وبيتا أندروفين، بالتالي تسريع معدلات التعلم وتحسين دورة النوم وتخفيف الآلام وإعطاء حساس بالراحة والتحسن. واعتبر موقع*(Psychology Today)* أنه يمكن استخدام هذه التقنية لعلاج القلق، أكثر تفاصيل حول الموضوع، يرجي زيارة الموقع الآتي: *http://www.tech-wd.com/wd/2014/11/15/%D8%A7%D9%84%D9%85%D8%AE%D8%AF%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A%D8%A9-digital-drugs-0/*،تاريخ الاطلاع:2016/02/06 على الساعة:10:47

[2] للمزيد من الاطلاع على هذا الموضوع الجديد، راجع الرابط الآتي: *https://ar.wikipedia.org/wiki/%D9%85%D8%AE%D8%AF%D8%B1_%D8%B1%D9%82%D9%85%D9%8A A*، تاريخ الاطلاع:2016/02/06 على الساعة:10:40،وأيضا، *http://www.alarabiya.net/ar/last-page/2014/10/30/%D8%A7%D9%84%D9%85%D8%AE%D8%AF%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A%D8%A9-%D8%AE%D8%B7%D8%B1-%D8%A5%D8%AF%D9%85%D8%A7%D9%86-%D8%AC%D8%AF%D9%8A%D8%AF-.html*، تاريخ الاطلاع:2016/10/07 على الساعة:11:18.

من الاسترخاء أو القوة عند الإنسان، بعدما تتسبب في إفراز غير طبيعي للمادة المنشطة للمزاج والتي قد تؤدي إلى تحطم الخلايا العصبية، والإصابة بالتشنجات أو الإعاقة العقلية. كما أنها تؤدى إلى الانعزال عن عالم الواقع والسعي لنشوة زائفة وكذلك حدوث عطب بالجهاز السمعي.

من جهة أخرى، عرف العالم العربي المخدرات الرقيمة سنة 2012، خاصة دولتي السعودية ولبنان، حيث تناقلت الأوساط السعودية تسجيل أول حالة وفاة جرّاء تعاطي "المخدرات الرقمية"، على الرغم من الجهود المبذولة للحد من وصول هذه المخدرات إلى المجتمع عبر الإنترنت، إلا أن وزارة الصحة أقرت بعجزها عن إمكان الوصول إلى معلومة من هذا النوع في وقتٍ قياسي، من جهتها دعت الحكومة اللبنانية بضرورة زيادة وعي الأهالي لمثل هذا النوع من المخدرات، ومراقبة ما يقوم به أولادهم على الإنترنت. كما دعت جهات حكومية لبنانية مختلفة لحجب المواقع الإلكترونية التي تقوم بتسويق وبيع هذه الموسيقى[1].

نظرا لخطورة أفعال الترويج والاتجار بالمخدرات والمؤثرات العقلية سواء في صورتها التقليدية أو في صورتها الجديدة المسماة بالمخدرات الرقمية –كما تم توضيحه سلفا– باستعمال شبكة الإنترنت لابد على المشرع الجزائري من التدخل باستحداث نصوص تجريميه صريحة لتدعيم سياسته الجنائية الهادفة إلى مكافحة كافة أشكال الجرائم الإلكترونية.

---

[1] أكثر تفاصيل حول الموضوع، يرجي زيارة الموقع الآتي: *http://www.tech-wd.com/wd/2014/11/15/%D8%A7%D9%84%D9%85%D8%AE%D8%AF%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A%D8%A9-digital-drugs-0/*، *تاريخ الاطلاع:2016/10/07 على الساعة:11:14.*

خلاصة الفصل الثاني:

تطرقنا في هذا الفصل إلى مكافحة الجرائم الإلكترونية بموجب قانون العقوبات وضمن بعض القوانين الخاصة، وأيضا بموجب (إ.ع.م.ج.ت.م) التي صادقت عليها الجزائر، أين تناولنا بعض الجرائم التي جاءت بها الاتفاقية ولم يجرمها المشرع الجزائري بعد.

أولا: بموجب قانون العقوبات: حيث قام المشرع الجزائري بتجريم الأفعال الماسة بالاعتبار والشرف مثل: جرائم الإهانة والسب والقذف سواء في حق الأشخاص مثل رئيس الجمهورية أو في حق مؤسسات الدولة، وذلك عن طريق استعمال الوسائل الإلكترونية أو المعلوماتية أو الإعلامية. والأمر نفسه قام به بخصوص جرائم المساس بحرمة الحياة الخاصة مثل: جريمة التقاط الأحاديث والصور دون رخصة. كما تناولنا أيضا أشكال الإرهاب الإلكتروني وخطره على أمن الدولة والأفراد على حد سواء.

ولكن تظل أكبر خطوة للمشرع هي تجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم:04-15 المؤرخ في:10 نوفمبر2004، بإضافة قسم سابع مكرر تحت عنوان" جرائم المساس بأنظمة المعالجة الآلية للمعطيات" من المواد(394 مكرر إلى 394مكرر7)، كجريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات، متماشيا في ذلك مع الاتجاه العالمي لمكافحة هذا النوع المستحدث من الجرائم بكافة أشكاله، حيث يهدف المشرع من وراء ذلك توفير الحماية الجزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات في ظل الطفرة التكنولوجية الهائلة في مجال تقنية المعلومات.

حيث استعمل المشرع مصطلح" منظومة " بدلا من مصطلح "نظام" لترك الباب مفتوحا في سياسته الجنائية أمام ظهور منظومات معلوماتية جديدة مع تعدد استعمالاتها. كما لم يشترط لقيام الجريمة خضوع النظام المعلوماتي للحماية الفنية، حيث يهدف المشرع من وراء ذلك إلى إضفاء الحماية الجزائية على كافة أنظمة المعالجة الآلية للمعطيات بغض النظر عن تمتعها بالحماية الفنية أم لا، إضافة إلى التوسّع في مفهوم الدخول غير المشروع ليشمل فعل الدخول والبقاء، وتجريم أفعال التلاعب في معطيات المنظومة المعلوماتية مثل: إدخال أو إزالة أو تعديل معطيات المنظومة ما لم يكن مصرحا بذلك. وهذا بقصد ضمان سريتها وسلامتها ووفرتها.

في المجال نفسه، وسّع المشرع من نطاق الحماية لتشمل كافة أنواع المعلومات وجميع وسائل التلاعب بها. كأفعال الاعتداء على سلامة المعطيات خارج المنظومة المعلوماتية عن طريق الحيازة والإفشاء والنشر والاستعمال...إلخ. كما نص على مضاعفة العقوبة تبعا لصفة المجنى عليه، وذلك

إذا مسّت هذه الجرائم الدفاع الوطني أو الهيآت والمؤسسات الخاضعة للقانون العام، وهو مسلك انفرد به المشرع الجزائري. إضافة إلى تبني المشرع مبدأ مسؤولية الشخص المعنوي الذي يرتكب هذه الجرائم وشدّد من العقوبة عليها. من جهة أخرى، وسّع أيضا من نطاق العقوبة، وذلك بتجريم الشروع والاتفاق الجنائي، والنص على العقوبات التكميلية كالمصادرة والغلق، وهو اتجاه محمود من المشرع لإضفاء فكرة الردع العام والخاص في ظل هذا الفضاء الافتراضي اللامحدود. كما يلاحظ تأثر المشرع الجزائري في وضعه للنصوص القانونية التي تحكم الجرائم الإلكترونية بكل من اتفاقية "بودابست للإجرام المعلوماتي"، والمشرع الفرنسي.

غير أننا نسجل بعض النقائص المتمثلة في إغفال المشرع النص على بعض الجرائم الأساسية التي تمس بأنظمة المعالجة الآلية للمعطيات كجريمة الاعتداء العمدي على سلامة وسير نظم المعالجة الآلية للمعطيات، حيث اكتفى بنصوص المواد(394 مكرر إلى 394 مكرر2)، حيث تعتبر هذه الجرائم شكلا آخرا من أشكال الاعتداء على المنظومة المعلوماتية. من جهة أخرى، لم يجرّم المشرع التزوير المعلوماتي، لذا على المشرع تدارك هذا الفراغ التشريعي من خلال استحداث نص خاص به أو بتوسيع مجال التزوير عن طريق توسيع مفهوم المحرر ليشمل أية دعامة أخرى على غرار التشريعات الحديثة ومنها التشريع الفرنسي. والأمر نفسه بخصوص عدم تجريم المشرع لأشكال الإرهاب الإلكتروني رغم ما يمثله من خطورة بالغة على أمن الدولة والأفراد. من جانب آخر لم ينص المشرع على تجريم المخدرات والمؤثرات العقلية التي تتم عبر شبكة الانترنيت(أفعال الترويج والاتجار...) خاصة ما استحدث منها كالمخدرات الرقمية *(cyber drugs)*. وعليه ندعو المشرع إلى تدارك هذا النقص التشريعي بما يحقق الفعالية في السياسة الجنائية للمشرع الجزائري بجانبيها الموضوعي والإجرائي في مكافحة هذا النوع المستحدث من الجرائم.

ثانيا: بموجب نصوص خاصة: في ظل توجه الدولة الجزائرية نحو الحكومة الإلكترونية، وما يفرضه ذلك من تحديات متعلقة بأمن المعلومات من حيث السرية والسلامة والتكامل والوفرة، وفي ظل وجود واقع محتشم للتجارة الإلكترونية في الجزائر مع عدم وجود تشريع خاص بها، ورغم ذلك وفّر المشرع قدرا من الحماية الفنية والجزائية -رغم نقصانها- لوسائل الدفع الإلكتروني، فمن خلال القانون رقم:2000-03 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاّسلكية، جرّم الأفعال الماسة بسرية ومضمون المراسلات بواسطة اللاّسلكي. وفي المجال نفسه، نص أيضا على جرائم المساس بالبطاقات الإلكترونية بموجب القانون رقم:08-01 المؤرخ في:2008/01/23 يتعلق بالتأمينات الاجتماعية، كما نص على الجرائم المتعلقة بالتوقيع والتصديق الإلكترونيين، وأضفى

عقوبات جزائية وإدارية على مرتكبيها، وهذا بموجب القانون رقم:15-04 المؤرخ في:2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

كما تطرقنا أيضا إلى جرائم تقليد المصنفات المعلوماتية بموجب الأمر رقم: 05/03 المؤرخ في 2003/07/19 يتعلق بحقوق المؤلف والحقوق المجاورة، تماشيا مع الحركة التشريعية العالمية التي اهتمت بحماية البرمجيات عن طريق حقوق الملكية الفكرية والأدبية.

وأخيرا تطرقنا إلى (إ.ع.م.ج.ت.م)، حيث تنص هذه الاتفاقية على جملة من الجرائم لم ينص عليها المشرع الجزائري بعد مثل: جريمة الاعتراض غير المشروع للبيانات وجريمة الإباحية الإلكترونية والتزوير المعلوماتي وتبييض الأموال وترويج وتجارة المخدرات عبر شبكة الإنترنت ومنها المخدرات الرقمية...إلخ. ونأمل أن يستدرك المشرع ذلك في أقرب الآجال بتحويل نصوص الاتفاقية إلى نصوص تشريعية لتعزيز سياسته الجنائية في مجال مكافحة الجرائم الإلكترونية.

الباب الثاني: الأحكام الإجرائية في مكافحة الجرائم الإلكترونية

تطرقنا في الباب الأول إلى الجوانب الموضوعية للجرائم الإلكترونية وما أثارته من مشكلات فيما يتعلق بإمكانية تطبيق النصوص التقليدية للقانون الجنائي على هذا النوع المستحدث من الجرائم احتراما لمبدإ شرعية التجريم والعقاب، وبرغم ذلك حاول المشرع الجزائري التصدّي لها عن طريق إفراد نصوص خاصة، تحيط بأركان الجريمة من كافة جوانبها ضمانا لعدم إفلات المجرم الإلكتروني من العقاب. لكن بالمقابل تثير هذه الجرائم المستحدثة في الوقت نفسه العديد من المشكلات في نطاق القانون الجنائي الإجرائي، حيث وُضعت نصوص قانون الإجراءات الجنائية لتحكم القواعد المتعلقة بجرائم تقليدية، لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم. وعلى العكس تماما تبرز صعوبات جمّة فيما يخص البحث والتحري وإثبات الجريمة الإلكترونية والوقاية منها على أساس أنها تتم في وسط افتراضي لا حدود له، وهو ما حاول أيضا المشرع الجزائري التكيّف معه في سياسته الجنائية الهادفة إلى مكافحة هذه الجرائم المستحدثة.

من هذا المنطلق ارتأينا تقسيم هذا الباب إلى فصلين، نتناول الإجراءات التقليدية والمستحدثة بخصوص جمع الدليل الإلكتروني ومدى حجيته في الإثبات الجنائي في(الفصل الأول)، ثم نتطرق إلى القواعد الخاصة للوقاية من الجرائم الإلكترونية في (الفصل الثاني).

الفصل الأول: إجراءات جمع الدليل الإلكتروني وحجيته في الإثبات الجنائي

دفعت الطبيعة الخاصة لهذه الجرائم المشرع الجزائري على غرار باقي المشرعين للبحث عن آليات وأساليب جديدة للبحث والتحري والإثبات لم تكن مستخدمة من قبل، فهي تستخدم التقنية نفسها التي يستعملها المجرم الإلكتروني، وذلك تماشيا مع التطورات التقنية التي عرفتها الجريمة الإلكترونية. كما تضمن في الوقت نفسه احترام حق الإنسان في الخصوصية المكفولة دستوريا وعدم الاعتداء على حرمة الحياة الخاصة للأفراد. كما شدّد على ذلك في التعديل الدستوري المؤرخ في:2016/03/06 [1]. وعليه قام المشرع الجزائري بتحديث المنظومة القانونية الإجرائية بموجب القانون رقم:06-22 المؤرخ في:2006/12/22 يعدل ويتمم قانون الإجراءات الجزائية، حيث نص على جملة من الإجراءات الجديدة في الفصل الرابع تحت عنوان: "في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" من المادة(65 مكرر 5 - 65 مكرر10)، كما نص أيضا في الفصل الخامس تحت عنوان: "في التسرّب" بموجب المادة(65 مكرر11 - 65 مكرر18)، وهي إجراءات جديدة تضاف

[1] المادتان(46 -47) من القانون رقم:16-01 يتضمن التعديل الدستوري.

إلى الإجراءات التقليدية مما يمكّن أجهزة التحقيق القضائي من الكشف على المجرم الإلكتروني في هذه البيئة الافتراضية التي يصعب التحقيق فيها بسبب طبيعتها الخاصة .

كما نصّ المشرع الجزائري أيضا في القانون رقم: 09-04 المؤرخ في: 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على جملة من الإجراءات الهامة خاصة ما تعلق بإجراءات التحقيق والتفتيش وحجز المعطيات والمساعدة القضائية، والاستعانة بكل شخص له دراية وخبرة لمساعدة جهات التحقيق في الكشف عن الجرائم الإلكترونية. فما هي هذه الأساليب المستحدثة في مجال التحقيقات القضائية الجنائية لمكافحة الجرائم الإلكترونية ؟ ولماذا اتسمت بطابع الخصوصية ؟ وهل تُحقّق الفعالية المطلوبة؟

وعليه سنتطرق إلى الإجراءات التقليدية لجمع الدليل الإلكتروني في (المبحث الأول)، ثم نتناول أساليب البحث والتحري المستحدثة في الكشف عن الجرائم الإلكترونية في (المبحث الثاني) لنختم في الأخير بالحديث عن حجية الدليل الإلكتروني في الإثبات الجنائي وموقف المشرع الجزائري من ذلك في (المبحث الثالث).

المبحث الأول: الإجراءات التقليدية لجمع الدليل الإلكتروني

يُعتبر التحقيق الابتدائي من أهم الإجراءات التي تُتخذ بعد وقوع الجريمة، لما له من أهمية في التثبّت من حقيقة الجريمة وأدلتها، لغرض الوصول إلى إدانة المتهم من عدمه. وعليه يعرف على أنّه:" مجموعة الإجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانونا بغية تمحيص الأدلة والكشف عن الحقيقة قبل مرحلة المحاكمة"[1]. ومن المعروف أن الدعوى الجزائية تمر بمرحلتين: مرحلة التحقيق ومرحلة المحاكمة، كما تنقسم مرحلة التحقيق أيضا إلى مرحلتين: مرحلة التحقيق الأولي(مرحلة التحري وجمع الاستدلالات) ومرحلة التحقيق الابتدائي[2]، ففي مرحلة التحقيق الأولي يتولى جهاز الضبطية القضائية مهام البحث والتحري وجمع وضبط أدلة الجريمة[3]، ومرحلة التحقيق

---

[1] عبد الرحمن خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، عين مليلة، الجزائر، 2010، ص157.

[2] تجدر الإشارة إلى أن بعض الشُرّاح ينتقدون تسمية التحقيق الأولي الذي يقوم به ضباط الشرطة القضائية بالتحقيق الابتدائي، انطلاقا من كون أن هذا المصطلح يرتبط أكثر بأعمال قاضي التحقيق وليس بأعمال الضبطية القضائية، وخلافا لهذا أضفى المشرع الجزائري مصطلح التحقيق الابتدائي على أعمال الضبطية القضائية بموجب المادة(15) والمادة (63) من (ق.إ.ج.ج) التي تنص على: "يقوم ضباط الشرطة القضائية وتحت رقابتهم أعوان الشرطة القضائية بالتحقيقات الابتدائية بمجرد علمهم بوقوع الجريمة إما بناء على تعليمات وكيل الجمهورية وإما من تلقاء أنفسهم". وفي الوقت نفسه تنص المادة (66) على أن:" التحقيق الابتدائي وجوبي في مواد الجنايات..." وبذلك يعتبر المشرع التحقيق الذي يمارسه ضباط الشرطة القضائية أو قضاة التحقيق، تحقيقا ابتدائيا على حد سواء.

[3] غالبا ما تبدأ الإجراءات الجزائية في الدعوى العمومية بمرحلة البحث والتحري أو مرحلة جمع الاستدلالات التي تتولاها أصلا الضبطية أو الشرطة القضائية، ولقد حدد (ق.إ.ج.ج) أحكام الضبط القضائي في المواد(12 إلى 28 و42 إلى 55 و63 إلى 65)، وتشمل==

الابتدائي يتولى فيها قاضي التحقيق الجمع بين أعمال ضباط الشرطة القضائية بحثا عن الحقيقة وبين أعماله كقاضي تحقيق يصدر عنه مجموعة من الأوامر ذات الطبيعة القضائية[1].

وعليه سنتطرق إلى بعض هذه الإجراءات التقليدية المتعلقة بجمع الدليل الإلكتروني، حيث سنتناول تلقي الشكاوى والبلاغات عبر الإنترنت في (المطلب الأول)، ثم نتطرق إلى كيفية الانتقال والمعاينة وإجراء الخبرة التقنية في البيئة الإلكترونية في (المطلب الثاني). بعدها نتعرف على أداء الشهادة في الجريمة الإلكترونية في (المطلب الثالث) لنختم في الأخير بالتطرق لحالة التلبس في الجريمة الإلكترونية في (المطلب الرابع).

المطلب الأول: تلقي الشكاوى والبلاغات عبر الإنترنت

يُناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقرّرة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها، وتعتبر صلاحية تلقى الشكاوى والبلاغات من المراحل المهمة في البدء في إجراء التحقيق الابتدائي[2]، خاصة في مجال مكافحة الجرائم الإلكترونية التي يصعب كشفها نتيجة وجود الدليل في بيئة رقمية يسهل معها محوه أو تدميره، كما تتعقد المهمة أكثر في حالة وجود الدليل الرقمي على خوادم تقع خارج إقليم الدولة[3]، إضافة إلى مشكلة إحجام المجنى عليه التبليغ عن الجرائم الإلكترونية نظرا لاعتبارات عديدة قد تكون شخصية متعلقة بالشرف والاعتبار أو اقتصادية متعلقة بالاتصال بالعملاء والشهرة.

سنتطرق إلى تلقى الشكاوى والبلاغات بالطرق التقليدية في (الفرع الأول)، ثم نتناول تلقي الشكاوى والبلاغات عبر شبكة الإنترنت في (الفرع الثاني).

الفرع الأول: تلقي الشكاوى والبلاغات بالطرق التقليدية:

أدّى التطور التقني الهائل في مجال تكنولوجيات الإعلام والاتصال إلى إساءة استخدام هذا الفضاء الافتراضي، مما نتج عنه أنماط جديدة للإجرام سواء من حيث الأساليب المستعملة أو نوعية

==الضبطية القضائية ضباط الشرطة القضائية وأعوانهم وبعض الموظفين المنوط بهم بعض مهام الشرطة القضائية، وعندما ينتهي ضابط الشرطة القضائية من مهمته يرسل محاضر البحث الأولى إلى وكيل الجمهورية الذي له حق التصرّف فيها.

[1] عبد الرحمن خلفي، المرجع السابق، ص159.

[2] في هذا الشأن نصت المادة (17) من (ق.إ.ج.ج) على: "يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12و13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية...". يتم في هذه المرحلة اكتشاف الجريمة وجميع عناصر التحقيق من طرف رجال الضبطية القضائية والأعوان والموظفون المبيّنون بالفصل الأول من الباب الأول من قانون الإجراءات الجزائية، حيث نصت المادة (14) على من يشملهم الضبط القضائي كضباط الشرطة القضائية وأعوان الضبط القضائي...إلخ.

[3] *Christiane Féral Schuhl, La collecte de la preuve numérique en matière pénale, Actualité Juridique Pénal, Editions Dalloz, 2009,p115.*

الجناة أو أصناف المجنى عليهم، مما صعّب كثيرا من عمل الأجهزة القضائية المختصة، خاصة في ظل عدم فعالية إجراءات التحقيق التقليدية التي لا تصلح للكشف عن هذا النوع من الجرائم وضبط مرتكبيها والتحفظ على أدلتها. وهو ما دفع بالمجلس الأوروبي اتخاذ جملة من التدابير الإجرائية في مجال مكافحة جرائم الحاسوب والإنترنت مثل: استقبال الشكاوى عبر الإنترنت، وتمديد إجراء تفتيش المنظومة المعلوماتية وحجز المعطيات، والحفظ السريع للمعطيات والتحكم في تقنيات التشفير بما يسهل مهمة أجهزة البحث والتحري...إلخ[1].

يعتبر تقديم الشكوى[2] والبلاغ بمثابة إشعارين لأجهزة السلطة القضائية بأن جريمة ما قد ارتكبت أو سترتكب لاحقا وعليهم التحرك فورا لمواجهتها بالانتقال إلى مكان حدوثها والحفاظ على الأدلة وتسجيل أقوال الشهود ...إلخ، في هذا الشأن نصت المادة (17) من (ق.إ.ج.ج) على: "يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12و13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالات وإجراء التحقيقات الابتدائية...". وعليه لم يحدّد القانون طريقة تقديم الشكوى من طرف الأشخاص المتضررين من الجريمة فقد تكون شفاهه كما قد تكون مكتوبة، وسواء كانت هذه الشكوى مقدمة من المضرور نفسه أو من محاميه[3]. أما البلاغات فتعني ما يرد إلى ضابط الشرطة القضائية من أخبار عن الجريمة سواء كانت شفاهه أو كتابة، بمعنى نقل العلم بوقوع حادث، أو جريمة إلى السلطة المختصة بناء على أسباب معقولة[4]. وعليه أوجبت المادة سالفة الذكر على مأموري الضبط القضائي قبول وتلقي الشكاوى والبلاغات التي ترد إليهم بشأن الجرائم وإرسالها فورا إلى النيابة العامة لتقرّر ما تراه مناسبا بشأنها.

كما نصت المادة (18) من (ق.إ.ج.ج) على: "يتعين على ضباط الشرطة القضائية أن يحرّروا محاضر بأعمالهم وأن يبادروا بغير تمهّل إلى إخطار وكيل الجمهورية بالجنايات والجنح التي تصل إلى علمهم...".

فإذا كان تلقى الشكاوى والبلاغات سواء شفاهه أو كتابة يبدو أمرا بسيطا في مجال مواجهة الجرائم التقليدية، فقد لا يكون الأمر كذلك حينما نكون أمام الجرائم الإلكترونية، حيث يُثار التساؤل حول مدى أهمية تلقي الشكاوى والبلاغات بواسطة الإنترنت ونظم المعلوماتية، وما هي القيمة

[1] *CHRISTIANE FERAL-SCHUHL, Le Droit à L'épreuve, 2e édition, Op.Cit,p.50.*

[2] يعرف الفقه الشّكوى بأنها: "إجراء يباشر من شخص معين وهو المجنى عليه، في جرائم محددة، يعبر به عن إرادته الصريحة في تحريك الدعوى العمومية لإثبات المسؤولية الجنائية وتوقيع العقوبة القانونية بالنسبة للمشكو منه"، عبد الرحمن خلفي، المرجع السابق ص119.

[3] محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007، ص59.

[4] المرجع نفسه، ص59.

القانونية لها؟ وهل تساعد فعلا في تسهيل اكتشاف الجرائم الإلكترونية ومن ثمة ملاحقة مرتكبيها؟ هذا ما سنتطرق إليه في الفرع الموالي.

الفرع الثاني: تلقّي الشكاوى والبلاغات عبر شبكة الإنترنت:

نظرا للطبيعة الخاصة للجرائم الإلكترونية، يمكن القول: بأنه لتلقى الشكاوى والبلاغات عبر شبكة الإنترنت أهمية بالغة في مجال مكافحة الجرائم الإلكترونية على المستوى الإجرائي، إذ يوفر لضباط الشرطة القضائية السرعة اللاّزمة في مباشرة إجراءات البحث والتحري بما يمكنّهم من الكشف المبكر عن الجريمة ومرتكبيه، وخاصة أن هناك إحجاما من طرف المتضررين في التبليغ عن الجرائم الإلكترونية لأسباب عديدة قد تكون شخصية أو إقتصادية...إلخ. كما أن لمكانة البلاغ في العالم المادي بنظيره الذي يتم عبر الإنترنت أهمية واحدة، ومن ثمة فإن تلقّي الشكاوى عبر الإنترنت له ذات الطبيعة التي عليها الحال في العالم المادي، حيث تتوافر نماذج للبلاغات عبر الإنترنت في عدة مواقع إلكترونية مثل: مواقع المباحث الفيدرالية الأمريكية والبوليس الإنجليزي والشرطة الفرنسية فيما يتعلق بجرائم الإنترنت[1]. في هذا المجال لم تكتف الدول المتقدمة بإجراء تلقي الشكاوى والبلاغات في صورتها التقليدية، بل قامت باستحداث أجهزة متخصصة لتلقي الشكاوي والبلاغات بواسطة شبكة الإنترنت واتخاذ الإجراءات اللاّزمة للكشف عن الجريمة وملاحقة مرتكبيها[2].

من جانب آخر، لازالت الدول المتخلفة تكنولوجيا متأخرة في مجال تلقى الشكاوى والبلاغات عبر شبكة الإنترنت لعدم وجود مواقع وأجهزة متخصصة، وحتى في حالة وجود مواقع للإبلاغ عن هذه الجرائم خاصة ما تعلق بالجرائم الإلكترونية، فإنه لا يتم تفعيل العمل بواسطتها لعدم وجود الإطارات المتخصصة ونقص الخبرة التقنية اللاّزمة لدى ضباط الشرطة القضائية في التعامل مع متطلبات الاستدلال والتحري في مجال الجرائم الإلكترونية، ناهيك على أن تقديم الشكوى أو البلاغ عبر الإنترنت يمكن أن يكون من شخص يستعمل اسما مستعارا أو صفة غير حقيقية أو أن الواقعة

---

[1] عمر محمد أبو بكر بن يونس، الرسالة السابقة، ص830.

[2] في هذا المجال طوّرت وكالات تطبيق القوانين أساليب وعلاقات جديدة للقبض على المجرمين في الفضاء السبراني، فظهر كنتيجة لذلك مركز الشكاوى الخاصة بجرائم الإنترنت *(IC3)* ، وهو كناية عن نظام تبليغ وإحالة لشكاوى الناس في الولايات المتحدة والعالم أجمع ضد جرائم الإنترنت، ويخدم المركز بواسطة استمارة للشكاوى مرسلة عبر شبكة الإنترنت حيث يقوم فريق من الموظفين والمحللين بتحويل الشكاوى والبلاغات إلى وكالات فرض تطبيق القوانين الأميركية والدولية التي تحقق في جرائم الإنترنت. حيث نشأ مركز الشكاوى الخاصة بجرائم الإنترنت كمفهوم سنة 1998 بعد ظهور جرائم الإنترنت خاصة في مجال الأعمال التجارية والمالية التي تتم عبرها ، ولأن مكتب التحقيقات الفدرالي أراد أن يكون قادراً على تعقب هذه النشاطات وعلى تطوير تقنيات سريعة للتحقيق في جرائم الإنترنت. كما يعمل هذا المركز مع وكالات أميركية ومنظمات دولية مثل: لجنة الجرائم الاقتصادية والمالية في نيجيريا *(EFCC)* ، زيدان زيبحة، مرجع سابق ص110، للاطلاع على تفاصيل أكثر، يرجى زيارة الموقع الرسمي للمركز العالمي للشكاوى الخاصة بجرائم الإنترنيت على الموقع الآتي: *https://www.ic3.gov/default.aspx، تاريخ الاطلاع:2016/09/2 على الساعة: 06:20.*

وهمية، وهو ما يتعارض مع كون الشكوى لا تقبل إلا من طرف الشخص المضرور[1]. إن قبول شكوى الشخص الذي يستعمل اسما وهميا أو مستعارا، والذي تعرض لجرائم البث العلني يفتح المجال واسعا أمام الجميع في التعامل بأسماء شخصيات وهمية، ومثل هذا الأمر يجعل استعمال الشخصية الوهمية مشروعة دائما[2]. حيث لا تكون الهوية المستعارة مشروعة إلا إذا كان القانون يجيز ذلك ومثال ذلك ما نص عليه المشرع الجزائري بخصوص إجراء التسرّب المتعلق بالبحث والتحري في بعض الجرائم الخاصة، ومنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات[3].

لقد رأينا سلفا أن المشرع الجزائري لم يشترط وسيلة محددة في تلقي الشكاوى والبلاغات فقد تكون كتابة أو شفاهه، بدليل تضمن نص المادة (17) من (ق.إ.ج.ج) لفظ: "... ويتلقون الشكاوى والبلاغات..."، وهو لفظ عام لم يحدد وسيلة بحد ذاتها يتم بها تلقى الشكاوى والبلاغات، مما يفتح المجال أمام القيام بهذا الإجراء بأي وسيلة كانت ومنها استعمال تقنية الاتصال متمثلة في شبكة الإنترنت والهاتف الخلوي...إلخ.

واستكمالا للسياسة الجنائية للمشرع الجزائري في مجال مكافحة الجريمة عموما والجريمة الإلكترونية خصوصا، قامت قيادة الدرك الوطني بإنشاء واطلاق خدمة عمومية جديدة عبر 48 ولاية باستعمال تكنولوجيات الإعلام والاتصال، تحت اسم " الشكوى المسبقة والاستعلام عن بعد ". حيث تدخل هذه الخدمة في إطار عصرنة وسائل تنفيذ مهام وحدات الدرك الوطني والتكفل الجيد بشكاوي المواطنين. وتأتي بهدف تعزيز العمل الجواري المنفذ من طرف الدرك الوطني لصالح المواطنين مستعملي الإنترنت خاصة في ظل الانتشار المتزايد للجرائم الإلكترونية بالاستفادة من تطور

---

[1] يُثار التساؤل حول مدى قبول الشكوى في جرائم البث العلني عبر الإنترنت مثل: الدردشة على مواقع التواصل الاجتماعي، وذلك في حالة استخدام الضحية هوية مستعارة أو في حالة انتحاله لاسم وهمي بقصد الإبحار الآمن. في هذا الصدد برز رأي مفاده قبول شكوى الضحية حينما يكون في حالة تخفي عندما يتعرض لجرائم البث العلني، حيث لا تهم شخصيته الوهمية مادامت الوقائع قد حدثت فعلا وبهذا الرأي أخذ القضاء الأسترالي في قضية راندوس وهاردويك *(RINDOS V.Hardwik)*، حيث اعتبرت المحكمة العليا لغرب استراليا بتاريخ:1994/03/31 أن بث نقد لاذع في حلقة نقاش لـ23000 مشترك في *(BBC)* خاصة بمؤسسة تعليمية متخصّصة يعد مظهرا من مظاهر التشهير، عمر محمد أبوبكر بن يونس، الرسالة السابقة، ص836.

[2] الرسالة نفسها، ص836.

[3] حيث نصت المادة (65 مكرر12) من (ق.إ.ج.ج) على :"يقصد بالتسرّب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف. يسمح لضباط أو عون الشرطة القضائية أن يستعمل، لهذا الغرض، هوية مستعارة...". وعليه أجازت المادة استعمال هوية مستعارة من طرف ضابط الشرطة القضائية بعد إذن وكيل الجمهورية، القيام بإجراء التسرّب في مجال البحث والتحري عن بعض الجرائم الخاصة ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فإذا تعرّض ضابط الشرطة القضائية لجرائم السّب أو إحدى جرائم البث العلني، فيحق له التقدم بشكوى بهويته المستعارة مع العلم أنه تعرض لذلك بمناسبة أداء مهامه، كون استخدام تلك الهوية كان مشروعا.

تكنولوجيات الإعلام والاتصال. حيث يمكّن هذ التطبيق المنجز من طرف مهندسي الإعلام الآلي للدرك الوطني المواطنين من إيداع البلاغات والشكاوى المسبقة عن طريق الإنترنت وتأكيدها بعد ذلك لدى وحدة الدرك الوطني المعنية في غضون 30 يوما، مما يمكّن أجهزة الضبطية القضائية من ربح الوقت والسرعة في البدء في إجراءات البحث والتحري بخصوص الكشف عن الجريمة الإلكترونية قبل أن يتمكن المجرم الإلكتروني من تدمير الدليل والإفلات من العقاب[1].

وإذا كان هذا الإجراء مستحسنا يمكّن الضحية من سهولة تقديم الشكوى والبلاغ خاصة في مجال الجرائم الإلكترونية، كما يمكن تطويره من خلال إمكانية تثبيت هذا التطبيق على الهواتف النقالة الذكية للوصول إلى أكبر شريحة من الناس، إلا أنه يبقى إجراء غير رسمي إلى غاية تأكيده من طرف الضحية في غضون 30 يوما، وهو فارق زمني كبير يتيح للمجرم الإلكتروني إمكانية محو الدليل ويخلق صعوبة بالغة في تتبعه، ناهيك عن المشكل المتعلق بسرية المعلومات المقدمة والمعطيات التي يقوم بإرسالها الشاكي، ومدى تأمينها لمنع الغير من الاطلاع عليها خاصة في حالة وقع اختراق من طرف الهاكرز للأنظمة المعلوماتية. فحبذا لو يتم اعتماده رسميا منذ لحظة إرساله من طرف الشاكي ربحا للوقت واستباقا للخطوات التي يمكن اتخاذها من طرف المجرم مثل: محو آثار جريمته.

المطلب الثاني: المعاينة والخبرة التقنية في البيئة الإلكترونية

يعتبر الانتقال والمعاينة من إجراءات التحقيق الهامة في المحافظة على آثار الجريمة والكشف عن مرتكبها خاصة ما تعلق بالجرائم التقليدية، إلا أنه يعتبر أقل أهمية في مجال الكشف عن الجرائم الإلكترونية نظرا للطبيعة الخاصة لهذه الأخيرة (الفرع الأول). من جانب آخر تعتبر الخبرة القضائية من طرق الإثبات المباشرة وذلك نظرا لاتصالها بالواقعة المراد إثباتها، ونظرا للطبيعة الخاصة للجرائم

---

[1] هذا التطبيق متوفر على الموقع الرسمي لقيادة الدرك الوطني على الإنترنت باللّغتين العربية والفرنسية، حيث يسمح للمستعمل الاختيار بين خدمتين، خدمة الشكاوى المسبقة أو خدمة المعلومات، ليتم بعد ذلك إدخال المعلومات وإرسالها إلكترونيا، وفي حالة تقديم شكوى مسبقة يتلقى صاحب الشكوى موعد عبر البريد الإلكتروني على مستوى وحدة الدرك الوطني المختصة إقليميا لتأكيد الشكوى، وذلك خلال 30 يوما وإتمام المحضر وفقا للإجراءات والقوانين المعمول بها. وهي تمكّن المواطنين من ربح الوقت بفضل حجز موعد مسبق لدى فرقة الدرك الوطني المختصة إقليميا، وتوفر أيضا إمكانية إرسال معلومات أو التبليغ عن أية جريمة مهما كان نوعها دون تكبّد عناء التنقل لمراكز الدرك الوطني. كما تعتبر هذه الوسيلة أداة فعّالة لتقديم خدمة عمومية ذات نوعية لفائدة المواطنين عبر 48 ولاية، وهي تأتي مسايرة لتطور وسائل وتكنولوجيات الإعلام والاتصال عبر العالم، للاطلاع أكثر حول تفاصيل هذه الخدمة الجديدة وشروطها، يرجي الدخول على الموقع الرسمي لقيادة الدرك الوطني على الرابط الآتي: *https://ppgn.mdn.dz/prep.php*، تاريخ الاطلاع:2016/09/10 على الساعة:07:29.

الإلكترونية من حيث جانبها الفني المتعلق بأساليب ارتكابها وسهولة إخفاء أو محو الدليل، بات من الضرورة استعانة جهات التحقيق أو القاضي بخبير متخصص في المعلوماتية لإنجاز خبرة رقمية بهدف استخلاص الدليل الإلكتروني، هذا ما سنتطرق إليه في (الفرع الثاني).

الفرع الأول: مفهوم الانتقال والمعاينة:

لم يتطرق المشرع الجزائري إلى مفهوم الانتقال والمعاينة، وبالرجوع إلى الفقه الجنائي، يعتبر الانتقال عملا هاما من أعمال التحقيق يتم بقصد جمع الأدلة وفحصها لكشف حقيقة الجريمة ويتطلب ذلك أن ينتقل المحقّق من مقر عمله إلى مكان آخر قد يكون مسرح الجريمة لإجراء عمل من أعمال التحقيق . حيث يتم الانتقال بهدف إجراء معاينة أو بهدف القيام بعمل آخر كالتفتيش والضبط وسماع أقوال الشهود في بعض الأحوال[1]. أما بخصوص المعاينة فهناك عدة تعاريف لها، فيقصد بها:" إثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة"[2] أو هي:" إثبات حالة الأشياء والأشخاص وغيرها وهي تستلزم الانتقال إلى محل وجود الشيء أو الشخص الذي ينبغي معاينته"[3].كما تعرف أيضا على أنها:" رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة"[4]، كما اعتبرها جانب من الفقه على أنها: "إثبات مباشر ومادي لحالة الأشخاص والأمكنة ذات الصلة بالحادث عن طريق رؤيتها أو فحصها فحصا حسيًّا مباشرا"[5].

وعليه تعتبر المعاينة عملية التوجه إلي مكان وقوع الجريمة والمحافظة عليه من أجل البحث وأخذ عيّنة من الآثار التي تركها المجرم، فهي عملية تنصب علي مسرح الجريمة وقد تقع علي دليل مادي أو جسم أو أحد أطراف الجريمة سواء كان الضحية أو المتهم. كما أنها تتوّج في الأخير بتحرير محضر كتابي مفصل لإثبات واقعة المعاينة، نظرا لأهميتها سواء لجهات التحقيق أو المحاكمة على حد سواء. كما يقوم بالمعاينة ضابط الشرطة القضائية ويساعده في ذلك الأخصائيون من الأقسام

---

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر ،2009 ، ص156.

[2] فؤاد حسن العزيزي، الجرائم المعلوماتية–دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، 2015، ص195، راجع أيضا، هبة حسين محمد زايد، الحماية الجنائية للصفقات الإلكترونية، دار الكتب القانونية، القاهرة، مصر، 2015، ص181.

[3] نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، شركة المؤسسة الحديثة للكتاب، طرابلس، لبنان، ط1 2011، ص151.

[4] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية–دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، مصر، ط1، 2009، ص208.

[5] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية–دراسة مقارنة، مكتبة الآلات الحديثة، مصر، 1994، ص57.

الفنية قصد كشف عناصر الجريمة وجمع أدلة الإثبات عن طريق حصر ومناظرة مكونات المكان الثابتة وموجوداته المنقولة من أجهزة وأدوات وآثار ناشئة عن وقوعها[1].

من جانب آخر لا تتمتع المعاينة في مجال كشف غموض الجريمة الإلكترونية بالدرجة نفسها من الأهمية التي تلعبها في مجال الجريمة التقليدية، وذلك مرده إلى قلة الآثار المادية التي تخلفها الجريمة الإلكترونية، ناهيك على أن عددا كبيرا من الأشخاص قد يتردّدون على مسرح الجريمة مما يتسبب في فقدان الأدلة[2].

كما يعني إجراء الانتقال والمعاينة في القانون الفرنسي وفق المواد (92-93) من (ق.إ.ج.ف)، جمع الأدلة المستمدة من الواقع *(Les indication tirés des faits)*، بمعني أن الدليل على وجود الجريمة يعد النتيجة الأولى من الملاحظة المباشرة سواء من معاينة المحقق أو قاضي التحقيق[3]. إن للمعاينة أهمية بالغة في الكشف عن الحقيقة حيث تتلخص في البحث عن العلاقة بين أثار الجريمة والإنسان الذي تركها وتسبب فيها، حيث تعتبر شاهدا شكليا وموضوعيا له وزنه في التحقيق. إن الأصل في المعاينة هي إجراء من إجراءات التحقيق[4]، باستثناء حالات التلبس بارتكاب جناية أين يجوز لضباط الشرطة القضائية القيام بالانتقال إلى مسرح الجريمة واتخاذ التحريات اللاّزمة[5]. كما يمكن للمحكمة أن تقوم بإجراء المعاينة إذا ما رأت في ذلك سبيلا لكشف الحقيقة سواء كان ذلك من تلقاء نفسها أو بناء على طلب الخصوم[6]. وحتى تأتي المعاينة بثمارها المرجوة سواء ما تعلق باكتشاف الأدلة أو إثبات حالة الأشخاص والأمكنة، نصت جل التشريعات[7] على توقيع

---

[1] خالد ممدوح إبراهيم، فن التحقيق، المرجع السابق، ص150.

[2] فؤاد حسين العزيزي، المرجع السابق، ص195.

[3] هبة حسين محمد زايد، المرجع السابق، ص184.

[4] حيث تنص المادة (79) من (ق.إ.ج.ج) على:" يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللاّزمة أو القيام بتفتيشها..."

[5] حيث تنص المادة (42) من (ق.إ.ج.ج) على:" يجب على ضابط الشرطة القضائية الذي بُلّغ بجناية في حالة تلبس أن يُخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية ويتخذ جميع التحريات اللاّزمة وعليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي وأن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة..."

[6] هبة حسين محمد زايد، المرجع السابق، ص182.

[7] حيث نصت المادة (43) من (ق.إ.ج.ج) على:" يحظر في مكان ارتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية... وإذا كان المقصود من طمس الآثار أو نزع الأشياء هو عرقلة سير العدالة عوقب على هذا الفعل بالحبس من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة من 1000 إلى 10.000دج".

جزاءات جنائية على كل من يحدث تغييرا أو تعديلا في مسرح الجريمة قبل قيام سلطات التحقيق بإجراء المعاينة[1].

مما سبق نستنتج: أنّ للمعاينة أهمية بالغة في الكشف عن الحقيقة في الجرائم التقليدية، إلا أن دورها ينحصر في مجال اثبات وقوع الجرائم الإلكترونية، ومرد ذلك إلى الاعتبارات الآتية[2]:

- إن الجرائم التي تقع على نظم المعلومات والشبكات قلما يخلف عن ارتكابها آثار مادية بسبب الطبيعة الخاصة لهذه الجرائم المستحدثة.
- تردد عدد كبير من الأشخاص على مسرح الجريمة خلال الفترة الزمنية الطويلة نسبيا بين ارتكاب الجريمة واكتشافها، مما يتسبب في حدوث تغيير أو اتلاف للآثار المادية بما يلقى ظلالا من الشك على الدليل المستمد من المعاينة.
- إمكانية التلاعب في البيانات عن بعد، أو محوها عن طريق التدخل من خلال وحدة طرفية من قبل المجرم الإلكتروني.

وحسنا فعل المشرع الجزائري حينما عاقب على المساس بمسرح الجريمة من كل شخص ليست له الصفة بموجب المادة (43) من (ق.إ.ج.ج) وكذا فعل نظيره المشرع الفرنسي بموجب المادة (55) من قانون (ق.إ.ج.ف)[3]، حيث كان الهدف هو الحرص على المحافظة على مسرح الجريمة من كل تصرف يؤدي إلى طمس آثار الجريمة قبل قيام أجهزة التحقيق بالمعاينة، تظهر أهمية ذلك خاصة في مجال الكشف عن الجرائم الإلكترونية إذ يتطلب الأمر سرعة التحرك لاستباق المجرم الإلكتروني قصد منعه من تعديل أو تدمير الدليل الإلكتروني.

فاذا كانت النصوص المنظمة للإجراء المتعلق بالانتقال والمعاينة تتصرف في أغلبها إلى الجرائم التقليدية، وإن كان يمكن تطبيقها بخصوص معاينة مكونات الحاسوب ذات الطابع المادي كالقرص الصلب والأشرطة والكابلات وشاشة العرض ...إلخ، إضافة إلى رفع البصمات وغيرها، ففي

---

[1] عفيفي كامل عفيفي، المرجع السابق، ص475.

[2] خالد ممدوح إبراهيم، فن التحقيق، المرجع السابق، ص154، لتفاصيل أكثر راجع، هبة حسين محمد زايد، المرجع السابق، ص ص 185-186.

[3] ***Article 55 du (CPPF) :***

"Dans les lieux où un crime a été commis, il est interdit, sous peine de l'amende prévue pour les contraventions de la quatrième classe, à toute personne non habilitée, de modifier avant les premières opérations de l'enquête judiciaire l'état des lieux et d'y effectuer des prélèvements quelconques…".

هذه الحالة ليس هناك صعوبات مادية فبإمكان ضابط الشرطة القضائية التحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة وضبطها ونسبتها إلى الفاعل مع إخطار النيابة العامة بذلك[1].

لكن بالمقابل يُثار التساؤل حول كيفية الانتقال إلى مسرح الجريمة الإلكترونية؟ وكيف يمكن معاينتها؟ وما هي الإجراءات الواجب اتخاذها حتى تأتي المعاينة بالنتائج المرجوة؟. هذا ما سنتعرف عليه فيما يأتي:

أولا: الانتقال والمعاينة التقنية لمسرح الجريمة الإلكترونية: قلنا آنفا أن مسرح الجريمة التقليدية يختلف عن مسرح الجريمة الإلكترونية نظرا للطبيعة الخاصة لهذه الأخيرة.

1- كيفية الانتقال إلى مسرح الجريمة الإلكترونية: تتم معاينة الجريمة الإلكترونية بالانتقال إلى مسرح الجريمة الإلكترونية[2]، غير أن الانتقال لا يتم بالضرورة عبر العالم المادي، وإنما عبر العالم الافتراضي*(Cyber Space)*. وعليه يستطيع ضابط الشرطة القضائية الانتقال إلى العالم الافتراضي لمعاينة الجريمة الإلكترونية كما يأتي[3]:

- يستطيع ضابط الشرطة القضائية الانتقال إلى العالم الافتراضي لمعاينة مسرح الجريمة من خلال حاسوبه الموجود بمكتبه.
- يمكن لضابط الشرطة القضائية اللّجوء إلى مقهى الإنترنت.
- يمكن لضابط الشرطة القضائية اللّجوء إلى مزود خدمة الإنترنت *(Internet Server Provider)* الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة.

2- المعاينة التقنية لمسرح الجريمة الإلكترونية: إن معاينة مسرح الجريمة الإلكترونية يختلف عن غيره من الجرائم بسبب طبيعة الدليل الإلكتروني غير المرئي والقابل للمحو، لذا ينبغي قبل الانتقال لمسرح الجريمة القيام بالخطوات الآتية:

---

[1] عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص211.

[2] يتكون مسرح الجريمة الإلكترونية من مسرحين:

الأول: مسرح تقليدي: يقع خارج بيئة الحاسوب ويتكون بشكل رئيسي من المكونات المادية للحاسوب، وهو أقرب ما يكون إلى مسرح أي جريمة تقليدية، فقد يترك الجاني آثارا كالبصمات وبعض المتعلقات الشخصية أو وسائط تخزين رقمية.

الثاني: مسرح افتراضي: يقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الإنترنت وفي ذاكرة الأقراص الصلبة للحاسوب. راجع، عائشة بن قارة مصطفى، المرجع السابق، ص84.

[3] نبيلة هبة هروال، المرجع السابق، ص218.

– توفير معلومات مسبقة عن مكان الجريمة، نوع وعدد الأجهزة وشبكات الاتصال الخاصة بها، قصد تحديد إمكانية التعامل معها فنيا[1].

– إعداد خريطة للموقع المتوقع الإغارة عليه والتأكد من تأمين وصلاحية الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة[2].

– إعداد فريق متخصص من الخبراء ورجال الأمن والضباط وإعطائهم الوقت الكافي للاستعداد فنيا عن طريق وضع خطة عملية لضبط أدلة الجريمة وقت معاينتها[3].

– الحصول على الاحتياجات الضرورية من أجهزة وبرامج للاستعانة بها في الفحص والتشغيل مثل: برامج معالجة الملفات*(Xtree Pro Gold)* وبرامج النسخ *(Lap Link)* وبرامج إنتاج صور مطابقة عن القرص الصلب *(Encase)*، والذي تستخدمه المباحث الفدرالية الأمريكية في التحقيقات الجنائية ويطلق عليه الخبراء(حقيبة الأدلة الرقمية)[4].

– تأمين عدم انقطاع التيار الكهربائي المفاجئ لأن ذلك يتسبب في محو المعلومات من الذاكرة، وبالتالي ضياع كافة العمليات التي تم تشغيلها واتصالات الشبكة وأنظمة الملفات الثابتة[5].

ثانيا: الإجراءات المتبعة أثناء المعاينة: قصد نجاح المعاينة لابد من مراعاة الجوانب الفنية الآتية:

– تصوير الحاسوب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز على تصوير الأجزاء الخلفية للحاسوب وتسجيل وقت وتاريخ ومكان التقاط كل صورة[6].

– العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام، واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، حتى يمكن إجراء عمليات المقارنة والتحليل[7].

– حصر أجهزة الحاسوب الموجودة في مكان المعاينة بصفة دقيقة، وفي حالة وجود شبكة للاتصالات، يجب البحث أولا عن خادم الملف *(File Server)* وذلك لأجل تعطيل حركة الاتصالات[8].

---

1 هبة حسين محمد زايد، المرجع السابق، ص186.

2 نبيلة هبة هروال، المرجع السابق، ص219..

3 عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص216.

4 عائشة بن قارة، المرجع السابق، ص85.

5 عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص217.

6 علي عدنان الفيل، إجراءات التحرّي وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الإسكندرية مصر، 2012، ص33.

7 هشام محمد فريد رستم، الجوانب الإجرائية، المرجع السابق، ص60.

8 عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص 218.

- عدم نقل أي معلومة من مسرح الجريمة، إلا بعد التأكد من خلو المحيط الخارجي لموقع الحاسوب من أي مجال مغناطيسي يمكن أن يتسبب في محول البيانات المسجلة[1].
- التحفظ على محتويات سلة المهملات، والقيام بفحص الأوراق والأشرطة والأقراص المضغوطة...إلخ[2].
- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسوب ذات الصلة بالجريمة[3].
- ربط الأقراص الكمبيوترية التي تحتوي على الأدلة مع جهاز يمنع الكتابة والتسجيل عليها بما يسمح للمحققين قراءة البيانات الموجودة فيها دون تعديلها[4].
- قصر مباشرة المعاينة على المحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة التقنية في مجال المعلوماتية واسترجاع المعلومات، والذين تلقوا تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يمكن أن يحتويها مسرح الجريمة الإلكترونية[5].
- ضبط وتحريز الدعائم الأصلية للبيانات وعدم الاكتفاء بضبط النسخ، كما يجب مراعاة ظروف تخزينها كعدم وضعها على مقربة من محطة إرسال لاسلكي أو وضعها في أماكن تحتوي على الغبار، بما يؤدي إلى إتلافها[6].
- منع أي إدخال جديد على الجهاز أو ذاكرته، وضبط برنامج التغذية الخاصة *(Software)* بالاستعانة بنظام التحميل *(Downloading)*[7].

على ضوء ما تقدم يمكن القول بعدم كفاية المعاينة كإجراء تقليدي للإحاطة بكافة جوانب مسرح الجريمة الإلكترونية نظرا لمميزات الدليل الإلكتروني، فهو غير مرئي كما يسهل على المجرم محوه أو تعديله بضغطة زر وفي جزء من الثانية وهو جالس وراء حاسوبه. لذا لنجاح المعاينة لابد من توفير فريق متخصص من ضباط الشرطة القضائية لديهم معرفة متميزة بالمعلوماتية عموما وبنظمها خصوصا وكيفية تشغيلها ووسائلها، وتقنيات إساءة استعمالها من قبل مستخدميها. ولا يتأتى ذلك إلا

---

[1] عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، من 12 إلى 14 نوفمبر 2007، الرياض، السعودية ص17.

[2] نبيلة هبة هروال، المرجع السابق، ص220.

[3] عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق، ص18.

[4] عائشة بن قارة، المرجع السابق، ص87.

[5] هشام محمد فريد رستم، الجوانب الإجرائية، المرجع السابق، ص61.

[6] خالد ممدوح إبراهيم، فن التحقيق، المرجع السابق، ص177.

[7] حسين براهيم، المقال السابق، ص87.

بتكوينهم وتدريبهم وتجديد معارفهم، قصد حصولهم على المهارات اللاّزمة في مجال الكشف عن الجرائم المستحدثة.

الفرع الثاني: الخبرة التقنية في العالم الافتراضي:

تعتبر الخبرة القضائية من طرق الإثبات المباشرة وذلك نظرا لاتصالها بالواقعة المراد إثباتها ونظرا للطبيعة الخاصة للجرائم الإلكترونية، من حيث طابعها الفني المتعلق بأساليب ارتكابها وسهولة إخفاء أو محو الدليل، بات من الضرورة استعانة جهات التحقيق أو القاضي بخبير متخصص في المعلوماتية لاستخلاص الدليل الإلكتروني. ومنه يطرح التساؤل حول أهمية الخبرة التقنية في مجال إثبات الجرائم الإلكترونية ومدى حجيتها؟، وهل تفي القواعد القانونية المنظمة لها بهذا الغرض؟ سنتطرق أولا إلى القواعد القانونية التي تحكم الخبرة القضائية بصفة عامة، ثم نتناول ثانيا الجوانب الفنية التي تحكم إنجاز الخبرة التقنية المتعلقة بإثبات الجريمة الإلكترونية.

أولا: القواعد القانونية التي تحكم الخبرة القضائية: للخبرة القضائية في التشريعات المعاصرة أهمية بالغة في الإثبات، وذلك لإسهامها في تحقيق العدالة وتنوير القاضي لأن لا يحيد في أحكامه على روح القانون. إن الاستعانة بالخبراء على تعددهم يتبين في الحالات التي يتعذر الوصول إلى الحقيقة لتوقّف الأمر على بعض النواحي الفنية التي تستلزم تدخلهم. وعليه تعد الخبرة في مجال المساعدة القضائية من أقوى مظاهر تعامل سلطات الاستدلال والتحقيق وأيضا المحاكمة مع الواقعة الإجرامية[1].

أ- **مفهوم الخبرة القضائية:** يعرّف جانب من الفقه المقارن الخبرة القضائية بأنها: "تنقيب وبحث يرتبط بمادة تتطلب معارف علمية أو فنية خاصة لا تتوافر سواء لدى المحقق أو القاضي"[2]. كما تعتبر الخبرة القضائية أيضا:" استشارة فنية يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى دراية علمية لا تتوافر لديه، والخبرة الفنية تعتبر إجراء من إجراءات التحقيق بحسب الأصل"[3]، أو هي: " إجراء يتعلق بموضوع يتطلب إلماماً بعلم أو فن معين لإمكان استخلاص الدليل منه، لذلك فإن الخبرة تفترض وجود شيء مادي أو واقعة يستظهر منه الخبير رأيه"[4].

---

1 عمر محمد أبوبكر بن يونس، الرسالة السابقة، ص1027.

2 هشام محمد فريد رستم، الجوانب الإجرائية، المرجع السابق، ص134.

3 عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق، ص24.

4 مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية المنعقد أيام: 23-25 / 9 / 2012، جمهورية السودان، 2012، ص32.

والعنصر المميز للخبرة عن غيرها من الإجراءات كالمعاينة والشهادة والتفتيش، هو الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها في الإثبات، والذي يتطلب معارف علمية وفنية خاصة لا تتوافر سواء لدى المحقق أو القاضي(1).

بالرجوع إلى المشرع الجزائري أجاز لجهات التحقيق وللمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم، حيث تنص المادة (143) من (ق.إ.ج.ج) على:" لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو الخصوم..."(2)، في حين حدد المشرع الهدف من إجراء الخبرة بموجب نص المادة (125) من قانون الإجراءات المدنية والإدارية رقم: 09-08 المؤرخ في 2008/02/25 التي تنص على:" تهدف الخبرة إلى توضيح واقعة مادية تقنية أو علمية محضة للقاضي"(3)، كما تجدر الإشارة إلى أنه ليس هناك اختلاف بين الخبرة القضائية عموما والخبرة التقنية من حيث القواعد القانونية المنظمة لها، إلا فيما يخص الجوانب الفنية التي تحكم عمل الخبير التقني، ورغم هذا هناك بعض التشريعات ومنها التشريع البلجيكي الذي نظم الخبرة التقنية في مجال الجرائم الإلكترونية بموجب قواعد خاصة(4).

ب- خطوات إنجاز الخبرة القضائية: تتم وفق الخطوات الآتية:

1-تعيين الخبير: اذا كانت الاستعانة بالخبير في الجرائم التقليدية أمر بالغ الأهمية في إثبات الجريمة، فإن الاستعانة به في مجال إثبات الجرائم الإلكترونية يعد أمرا متطلبا وضروريا بسبب التطور التقني السريع في مجال تقنية المعلومات، إذ لا يكشف غموض الجريمة إلا من طرف شخص

---

1 خالد ممدوح ابراهيم، فن التحقيق، المرجع السابق، ص284.

2 المواد (143-156) من (ق.إ.ج.ج).

3 تهدف الخبرة التقنية في الجرائم الإلكترونية إلى:

- الكشف عن الدليل الرقمي.
- إجراء الاختبارات التكنولوجية والعلمية على الدليل الرقمي للتأكد من أصالته وصلاحيته ومصدره لتقديمه كدليل لأجهزة إنفاذ القانون.
- إصلاح الدليل وإعادة تجميعه من المكونات المادية للحاسوب*(Hard Drive)*.
- عمل نسخ أصلية عن الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.
- جمع الآثار المعلوماتية الرقمية *(Cyber Trial Digital)* التي قد تكون تبدلت خلال الشبكة المعلوماتية.
- استخدام الخوارزميات *(Algorithmes)* للتأكد من أن الدليل لم يتم العبث به أو تعديله، راجع، خالد ممدوح إبراهيم، فن التحقيق، المرجع السابق، ص ص302-303.

4 حيث تنص المادة (88) من القانون البلجيكي الصادر في: 2000/11/23 على:" يجوز لقاضي التحقيق وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته"، راجع، علي عدنان الفيل، المرجع السابق، ص30.

على درجة كبيرة من العلم والدراية في مجال تخصّصه[1]، حيث يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة، كما تحدد الأوضاع التي يجري فيها قيد الخبراء أو شطبهم بقرار من وزير العدل[2]. فمن جهة ترك المشرع للقاضي حرية ندب خبير واحد أو خبراء متعددين وذلك بموجب المادة (147) من (ق.إ.ج.ج). ومن جهة أخرى لم يحدد المشرع الجزائري طبيعة الشخص الخبير فيمكن أن يكون شخصا طبيعيا أو شخصا معنويا كمؤسسة متخصصة في مجال تقنية المعلومات.

2-حلف اليمين: كما أوجب المشرع الجزائري لضمان صحة تقرير الخبير ونيل ثقة أطراف الدعوى، أن يحلف اليمين[3] قبل البدء في إنجاز الخبرة.

3- الخضوع للرقابة القضائية: عندما يباشر الخبير مهمته فهو تحت رقابة قاضي التحقيق أو القاضي الذي أمر بإجراء الخبرة، ولا يستلزم حضوره الفعلي ويكفي أن يبقى على اتصال بالقاضي[4].

4-إنجاز الخبير لأعمال الخبرة بنفسه: لا بد على الخبير أن يقوم بأعمال الخبرة بنفسه وفي حدود ما نص عليه أمر أو حكم الندب، وأن يستجيب لطلبات التي يقدمها أطراف الخصومة مثل: سماع أي شخص قادر على إعطاء معلومات فنية[5].

5-إيداع الخبرة التقنية: بعد انتهاء الخبير من أعماله التي كُلّف بها، يقوم بإيداع الخبرة التقنية خلال المدة المحددة في أمر أو حكم الندب، وأن يقدم نتائج ما قام به من أبحاث فإن خالف ذلك جاز للقاضي استبداله بغيره، كما يمكن أن يتخذ في حق الخبير الذي ثبت وقوع إهمال منه إجراءات تأديبية قد تصل إلى شطب اسمه من جداول الخبراء بقرار من الوزير[6].

---

1 *David FOREST et Gautier Kaufman,Op.cit,pp.79-80.*

2 حيث تنص المادة (144) من (ق.إ.ج.ج) على:" يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة، وتحدد الأوضاع التي يجري بها قيد الخبراء أو شطب أسمائهم بقرار من وزير العدل...".

3 حيث تنص المادة (145) من (ق.إ.ج.ج) على:" يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتية بيانها: أقسم بالله العظيم بأن أقوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص وأن أبدي رأيي بكل نزاهة واستقلال. ولا يجدد هذا القسم مادام الخبير مقيّدا في الجدول...".

4 المادة (4/143) من (ق.إ.ج.ج).

5 المادة (152) من (ق.إ.ج.ج).

6 حيث تنص المادة (148) من (ق.إ.ج.ج) على:" كل قرار يصدر بندب خبراء يجب أن تحدد فيه مهلة لإنجاز مهمتهم ويجوز أن تمدد هذه المهلة بناء على طلب الخبراء إذا اقتضت ذلك أسباب خاصة ويكون ذلك بقرار مسبب يصدره القاضي أو الجهة التي ندبتهم. وإذا لم يُودع الخبراء تقاريرهم في الميعاد المحدد لهم جاز في الحال أن يستبدل بهم غيرهم وعليهم إذ ذاك أن يقدموا نتائج ما قاموا به من أبحاث. كما عليهم أيضا أن يردوا في ظرف ثمان وأربعين ساعة جميع الأشياء والأوراق والوثائق التي تكون قد عهد بها إليهم على ذمة إنجاز مهمتهم...ويجوز دائما لقاضي التحقيق أثناء إجراءاته أن يستعين بالخبراء إذا رأى لزوما لذلك".

ثانيا: مدى حجية الخبرة التقنية: بعد إيداع الخبير للخبرة التقنية المنجزة، وبالرجوع إلى نص المادة 215 من (ق.إ.ج.ج) التي تنص على:" لا تعتبر المحاضر والتقارير المثبتة للجنايات أو الجنح إلا مجرد الاستدلالات ما لم ينص القانون على خلاف ذلك"، تعتبر هذه الخبرة مجرد استدلالات لإنارة القاضي، بسبب أن رأي الخبير يعطي بصفة استشارية وليس له أي قوة ملزمة. حيث أعطى المشرع لمحكمة الموضوع كامل الحرية في تقدير القوة التدليلية لتقرير الخبير المقدم، كما أن المحكمة لا تلتزم في أصول الاستدلال بالتحدث في حكمها إلا عن الأدلة ذات الأثر في تكوين عقيدتها، فلها أن تفاضل بين تقارير الخبراء وتأخذ بما تراه وتطرح ما عداه إذ أن الأمر يتعلق بسلطتها في تقدير الدليل واعمالا لمبدأ "القاضي خبير الخبراء"[1].

غير أن إعمال مبدأ "القاضي خبير الخبراء" الذي ظل مستقرا نسبيا يتعرض لهزات عنيفة إزاء التزايد المتواصل لمبدأ التفاعل القانوني مع الظواهر العلمية التي تقع في اختصاص آخر غير الجوانب النظرية، حيث لا تسمح ثقافة القاضي المبنية على معايير العدالة والدراسات القانونية من التفاعل معها مثل: التعامل مع التكنولوجيا الحديثة في مجال تقنية المعلومات وشبكة الإنترنت والجرائم الناتجة عنها، حيث تفرض على القاضي الاستعانة المطلقة بالخبير، وهو تصرف منطقي من القاضي، حيث أن رأي الخبير ورد في موضوع فني وتقني بحت لا علم للقاضي فيه[2].

ثالثا: الجوانب الفنية التي تحكم إنجاز الخبرة التقنية: قلنا سلفا أن ما يميز الجريمة الإلكترونية عن غيرها، هو أنها من جهة ترتكب في مسرح إلكتروني أو مجال مفرغ يختلف كلياً عن المسرح التقليدي للجريمة، ومن جهة أخرى تتعدد مجالات الخبرة الرقمية بالنسبة للجرائم الإلكترونية[3]. وعليه يختلف الأمر من حيث توافر بعض الشروط في الخبير، إضافة إلى اتخاذ اجراءات خاصة تتلائم وطبيعة جمع الدليل في البيئة الإلكترونية، وهو ما سنتطرق إليه كما يلي:

1- بالنسبة للخبير: إن المشكلة التي تواجه نظم إجراء الخبرة التقنية عموما تتمثل في تكوين الخبير الذي يستعان به، ذلك أن الاستعانة بالخبرة في مجال الكشف عن الجرائم الإلكترونية على اختلاف أنواعها لا يعتمد فقط على شهادة الخبير الذي تتوفر فيه الشروط الشكلية والموضوعية

---

[1] رشيدة بوكر، المرجع السابق، ص429، راجع أيضا، عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق، ص ص29-30.

[2] عمر محمد أبوبكر بن يونس، الرسالة السابقة ، ص1028.

[3] تقوم الأنشطة الحديثة كالتجارة الإلكترونية والبنوك والأعمال المصرفية الإلكترونية والحكومة الإلكترونية على استخدام تقنية المعلومات التي قوامها شبكة الإنترنت ونظم وبرمجيات الحاسوب، مما يترتب عليه تنوع الجرائم التي ترتكب على هذه الأنشطة، وبالتالي تعدد الخبرات الرقمية مثل: تزوير المستندات المدخلة في الحاسوب والمخرجة منه بعد المعالجة، التلاعب في البيانات، التلاعب في البرامج الأساسية والتطبيقات، والغش أثناء نقل وبث البيانات، راجع، هشام محمد فريد رستم، الجوانب الإجرائية، المرجع السابق، ص ص137-140.

التقليدية المتطلبة في الخبير، وإنما يتطلب الأمر أيضا شروطا أخرى تتناسب والتطورات الحاصلة في مجال تقنية المعلومات والجرائم المرتبطة بها[1]. وعليه يتطلب في الخبير في مجال الخبرة التقنية المتعلقة بالجرائم الإلكترونية، أن يكون لديه إلمام كاف بالجوانب الفنية والتقنية في مجال تكنولوجيا المعلومات نذكر منها[2]:

- معرفة تركيب الحاسوب ونوعه وطرازه .
- معرفة أنواع نظم التشغيل والأنظمة الفرعية المستخدمة بالإضافة إلى الأجهزة الطرفية الملحقة.
- بيئة الحاسوب أو الشبكة من حيث طبيعتها، تركيزها أو توزيعها، وكذا نمط ووسائل الاتصالات.
- خبرة فنية حول اختراق كلمات المرور ونظم التشفير.
- معرفة شاملة لشبكة الإنترنت.
- المكان المحتمل لأدلة الإثبات وشكلها وهيئتها.
- كيفية عزل النظام المعلوماتي والحفاظ على الأدلة دون تلف.
- الكيفية التي يتم بواسطتها نقل الأدلة إلى الأوعية دون إتلافها.
- كيفية تجسيد الأدلة في صورة مادية، وذلك بنقلها إن أمكن إلى أوعية ورقية تتيح للقاضي مطالعتها وفهمها مع الإثبات أن المطبوع على الورق هو مطابق لما هو موجود على الدعامة الممغنطة.

2- بالنسبة للإجراءات: قبل البدء في إنجاز الخبرة، لا بد على الخبير القيام بالخطوات الضرورية الآتية[3]:

أ- ما قبل التشغيل والفحص: تتمثل في ما يأتي:

- التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدوّن عليها.
- التأكد من صلاحية وحدات نظام التشغيل.
- تسجيل بيانات الوحدات المضبوطة، ويتم ذلك عبر تسجيل نوع الوحدة والطراز والرقم التسلسلي وتاريخ ومكان الصنع...إلخ.

---

1 عمر محمد أبوبكر بن يونس، الرسالة السابقة، ص1033.

2 عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص99 ، راجع أيضا، علي عدنان الفيل، المرجع السابق، ص ص29-30 ، وأيضا، هشام محمد فريد رستم، الجوانب الإجرائية، المرجع السابق، ص142.

3 رشيدة بوكر، المرجع السابق، ص ص430-431، راجع أيضا، خالد ممدوح ابراهيم، فن التحقيق، المرجع السابق، ص ص308-309.

ب- التشغيل والفحص: تتمثل في ما يلي[1]:

- استكمال تسجيل باقي بيانات الوحدات من خلال قراءات الحاسوب.
- عمل نسخ مطابقة للأصل عن كل من وسائط التخزين المضبوطة كالقرص الصلب لحماية الأصل من الفقد أو التلف أو التدمير.
- تحديد أسماء وأنواع مجموعات البرامج، مثل: برامج النظام وبرامج التطبيقات وبرامج الاتصالات وما إذا كان هناك برامج ذات دلالة بموضوع الجريمة كالمستندات، ووجود رسائل تهديد في البريد الصادر ...إلخ.
- إظهار الملفات المخبأة والنصوص المخفية داخل الصور واستخدام برامج استعادة البيانات.
- تحويل الدليل الرقمي إلى هيئة مادية عن طريق طباعة الملفات أو تصوير محتواها.
- تخزين الملفات والمعطيات وعمل نسخ أصلية عنها تفاديا لضياعها.

وعليه يقوم الخبير بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في حد ذاتها، ثم يقوم بتحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه، ومن ثمة التوصل في النهاية إلى معرفة بروتوكول الإنترنت*(IP)* الذي ينسب إلى جهاز الحاسوب الذي صدرت عنه الجريمة. كما يقوم الخبير أيضا بتحصيل مجموعة الموقع التي لا يشكل موضوعها جريمة في حد ذاته، وإنما تؤدي حال تتبعها إلى قيام الأفراد بارتكاب جرائم إلكترونية.

رابعا: موقف المشرّع الجزائري: أدرك المشرع الجزائري خصوصية الجريمة الإلكترونية وصعوبة التحقيق فيها، لذا حاول وضع نصوص قانونية تسهل وضع ترتيبات لإجراء الخبرة الرقمية وذلك على عدة مستويات:

أ- على مستوى تعيين الخبراء: كما رأينا سلفا، نلاحظ أن المشرع الجزائري ترك المجال مفتوحا أمام جهات التحقيق والقضاة حول إمكانية الاستعانة بالخبير الاستشاري من خارج الجدول القضائي نظرا لخصوصية الجريمة الإلكترونية ولصعوبة التحقيق فيها، ولإدراكه بأهمية التطور التكنولوجي السريع في مجال تكنولوجيات الإعلام والاتصال، ناهيك على إمكانية عدم توفر كفاءات وخبرات عالية ضمن الخبراء المقيّدين في الجداول . حيث تنص المادة (144) من (ق.إ.ج.ج) على: "يختار الخبراء من الجدول الذي تعده المجالس القضائية... ويجوز للجهات القضائية بصفة استثنائية أن تختار بقرار مسبب خبراء ليسوا مقيدين في أي من هذه الجداول". ويستوي أن يكون هذا الخبير شخصا طبيعيا أو معنويا والعبرة بتوافر المعرفة العلمية والخبرة اللاّزمتين في مجال تكنولوجيا المعلومات التي تتطور بصورة مذهلة.

---

[1] محمد فتحي محمد أنور عزت، المرجع السابق، ص ص430-431.

وفي السياق نفسه، أجاز المشرع لجهات التحقيق أثناء تفتيش المنظومة المعلوماتية الاستعانة بكل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، وهذا بموجب المادة (05) من القانون رقم: 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تنص على:"...يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها". حيث لم يحدد المشرع طبيعة هذا الشخص فقد يكون شخصا طبيعيا أو معنويا، كما قد يكون خبيرا أو شخصا عاديا، ولكنه يملك مهارات وقدرات عالية في مجال من مجالات تكنولوجيا الإعلام والاتصال. في هذا الشأن ونظرا للطبيعة الخاصة للجرائم الإلكترونية، وفي إطار الاتفاق مع الجهات القضائية المختصة، يمكن الاستعانة بالقراصنة الذين أنهوا عقوبتهم أو تمت تبرئة ساحتهم، قصد الكشف عن الجريمة الإلكترونية ومرتكبيها، نظرا للمهارات والخبرات الاستثنائية التي يمتلكونها في مجال تقنية المعلومات وشبكة الإنترنت، وقد يكون هذا سبيلا لإعادة إدماجهم في المجتمع.

ب-على مستوى إنشاء الهيآت: نص المشرع الجزائري على إنشاء هيآت بكوادر مؤهلة تقوم بإجراء الخبرة الرقمية سواء بمناسبة إجراء تحقيق أو المساعدة على إجرائه وذلك كما يلي:

- إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي[1]، حيث تم تنظيم المصالح والأقسام والمخابر لذات المعهد بموجب قرار وزاري مشترك تضمن 05 مخابر جهوية، يحتوي كل مخبر على مصلحة تقنية تضم بدورها 06 مخابر من بينها مخبر الأدلة المعلوماتية وجرائم الكمبيوتر إضافة إلى مخبر استغلال الهواتف المحمولة[2].

- إنشاء قيادة الدرك الوطني للمركز الوطني لمكافحة الجريمة المعلوماتية الموجود "ببئر مراد رايس" بالجزائر العاصمة، مهمته تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها، وكذا تأمين الأنظمة المعلوماتية.

---

[1] المرسوم الرئاسي رقم:04-432 المؤرخ في:12/29/ 2004 يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، حيث نصت المادة (05) منه على:" يتولى المعهد المهام الآتية:...إعداد تقارير الخبرة بناء على طلب من السلطات المختصة المؤهلة قانونا- القيام بأعمال التكوين وتجديد المعارف وتحسين المستوى والتكوين ما بعد التدرج في ميداني علم التحقيق الجنائي والإجرام..."، (ج. ر) رقم:84 المؤرخة في:2004/12/29، ص25.

[2] القرار الوزاري المشترك المؤرخ في:2007/04/14، يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، (ج.ر) رقم:36 المؤرخة في:03 يونيو 2007، ص ص14-18.

– إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام[1]، وهي مؤسسة عمومية ذات طابع إداري تشكل أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة، يقدم خدمات أساسية في مجال خدمة العدالة ودعم وحدات التحرّي في إطار مهام الشرطة القضائية، من مهامه:

- القيام بالخبرات العملية أو الخبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة من أجل كشف الحقيقة بالأدلة العلمية لتحديد هوية مرتكبي الجنايات والجنح.
- مساعدة المحققين للسير الحسن للمعاينات، خاصة عن طريق الوضع تحت تصرف الأفراد المؤهلين أثناء الحاجة.
- تنفيذ مناهج الشرطة العلمية والتقنية، لجمع وتحليل الأدلة المأخوذة من مسرح الجريمة.
- ضمان المساعدة العلمية في التحريات المعقدة، والمشاركة في الأبحاث والتحاليل المتعلقة بالوقاية للتقليل من كافة أشكال الإجرام.
- مشاركة المعهد الوطني للأدلة الجنائية وعلم الإجرام بصفته الهيئة المزودة بالتحاليل والخبرات في ميدان علم الإجرام، والمساهمة في إنجاز سياسة مكافحة الإجرام.

– إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث أُسندت إليها مهمة إنجاز الخبرة الرقمية في مجال مكافحة الجرائم الإلكترونية، وهذا بموجب نص المادة (14/ب) من القانون رقم:09-04 سالف الذكر[2]. كما أكدت المادة (5/04) من المرسوم الرئاسي رقم:15-261 المؤرخ في:2015/10/08 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على مهام الهيئة ومن بينها إجراء الخبرة القضائية في مجال مكافحة الجرائم الإلكترونية[3].

وفي الأخير يمكن القول: أن المشرع الجزائري نظّم إلى حد ما إنجاز الخبرة الرقمية بما يتوافق وطبيعة الجرائم الإلكترونية، غير أن المشكلة تكمن في التطور السريع في مجال تكنولوجيات الإعلام والاتصال يقابله تطور أيضا في أساليب وأدوات ارتكاب الجرائم المرتبطة بها، لذا لا بد من الاهتمام

---

[1] المرسوم الرئاسي رقم: 183-04 المؤرخ في : 26 جوان 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، (ج. ر) رقم:41 المؤرخة في:2004/06/27، ص18.

[2] نص المادة (14/ب) من القانون رقم: 09-04 على:" ...مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية...".

[3] المادة (5/04) من المرسوم الرئاسي رقم:15-261 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

بالتكوين النظري والتدريب العملي للمكلفين من السلطة القضائية المختصة بالتحقيق في الجرائم الإلكترونية[1] قصد تجديد المعارف وتحسين المستوى واكتساب المهارات التقنية اللاّزمة والاستفادة من خبرات الدول الرائدة في هذا المجال، ناهيك عن توفير الوسائل الحديثة في مجال تكنولوجيات الإعلام والاتصال[2].

المطلب الثالث: الشهادة في الجريمة الإلكترونية

يعتمد القانون الجزائري على غرار سائر القوانين جملة من وسائل الإثبات، منها الإقرار والخبرة ثم المعاينة والتفتيش وكذا شهادة الشهود التي تكتسي أهمية بالغة في مجال الإثبات الجنائي، لأن الجريمة ليست تصرفا قانونيا، ولكنها عمل غير مشروع، يجتهد الجاني في إخفائه عن الناس. إن الشهادة في مجال الجرائم الإلكترونية لا تختلف من حيث ماهيتها عنها في الجرائم التقليدية، سنتناول مفهوم الشهادة والشاهد في الجريمة الإلكترونية في (الفرع الأول)، ثم الالتزامات الواقعة على عاتق الشاهد المعلوماتي في (الفرع الثاني).

الفرع الأول: مفهوم الشهادة والشاهد المعلوماتي:

سنتطرق إلى مفهوم الشهادة وأهميتها كوسيلة في الإثبات الجنائي، ثم نتناول مفهوم الشاهد المعلوماتي.

---

[1] لمزيد من التفاصيل حول التدريب وأهميته في مجال مكافحة الجرائم الالكترونية، راجع، حسين بن سعيد الغافري، السياسة الجنائية المرجع السابق، ص ص678-682.

[2] في إطار المجهودات المبذولة من طرف السلطة القضائية بالجزائر، بخصوص تدريب وتكوين ضباط الشرطة القضائية والقضاة في مجال البحث والتحري عن الجرائم الإلكترونية، أشرف خبراء من الاستخبارات المركزية الأمريكية *(CIA)* وعملاء من مكتب التحقيقات الفدرالي*(FBI)*، على ورشة تكوينية حول مكافحة الجريمة المعلوماتية لفائدة ضباط الشرطة القضائية والقضاة، تهدف إلى اطلاعهم على آخر التكنولوجيات لمحاربة الجريمة وكيفية استخدام الأدلة الإلكترونية في التحقيق والمقاضاة. شارك في الإشراف على الورشة التدريبية خبراء من مكتب التدريب والمساعدة لتطوير المقاضاة عبر البحار قسم الجرائم الحاسوبية والملكية الفكرية، قسم الجريمة المنظمة وابتزاز الأموال التابعة لوزارة العدل الأمريكية. حيث استفاد من هذه الورشة التدريبية 10 ضباط من الشرطة القضائية و60 قاضيا متخصصا في الجريمة المنظمة في الجزائر، تلقوا تدريبات نظرية وتطبيقيا عبر التعرف على تقنيات إجراءات التحري وإقامة الدليل على الجرائم المعلوماتية، وعلاقة الجريمة المعلوماتية بالجريمة المنظمة وأمن المعلومات والمعطيات وكيفية استغلال الإنترنت والبريد الإلكتروني، وكذا التعاون الدولي في هذا المجال، عثمان لحياني، ورشة حول الجريمة الإلكترونية وأمن المعلومات، مقال منشور على الموقع الرسمي لمحرك البحث الإخباري الجزائري جزايرس *(djazairess)*على الرابط الآتي: *http://www.djazairess.com/elkhabar/235287* ، تاريخ الاطلاع:2016/04/01 على الساعة:09:24.

أولا: مفهوم الشهادة: لم يتطرق المشرع الجزائري إلى تعريف الشهادة وترك ذلك للفقه والاجتهاد القضائي، لكنه بالمقابل قام بتنظيمها وتحديد مجالها وشروط قبولها وحجيتها في الإثبات[1]. فيعرفها جانب من الفقه على أنها:" الأقوال التي يُدلي بها غير الخُصوم أمام سلطة التحقيق بشأن جريمة وقعت، سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم أو براءته منها"[2]، أو هي :" تقرير شخصي في شأن واقعة معينة عاينها بحاسة من حواسه سواء البصر أو السمع أو الشم أو غيرها"[3]، كما تعني أيضا:" الإدلاء بمعلومات تتعلق بالجريمة أمام سلطة التحقيق بالشروط التي حددها القانون"[4].

فالشهادة هي إقرار من الشاهد بأمر رآه أو سمعه أو أدركه بأية حاسة من حواسه، فعندما تعرض القضية على جهات التحقيق يمكن اللّجوء إلى سماع الشهود ومناقشتهم ومواجهتهم بالمتهم حول جزئيات القضية، كما يمكن لخصوم الدعوى أيضا المطالبة بسماع شهادة بعض الأشخاص قد تكون معلوماتهم ذات أثر في نفي أو إثبات الواقعة[5].

أما في مجال الجرائم الإلكترونية فيقصد بالشهادة: "هو ذلك الشخص المتخصص في مجال المعلوماتية، والذي يستطيع وبطلب من الجهات القضائية المختصة، الولوج إلى نظام المعالجة الآلية للمعطيات بهدف الحصول على الأدلة الرقمية"[6]. من ناحية أخرى تنقسم الشهادة إلى عدة أقسام: فهناك الشهادة المباشرة وغير المباشرة والشهادة الشفهية والمكتوبة والشهادة بالتسامع، إضافة إلى ظهور نوع مستحدث يسمى بالشهادة الإلكترونية عن بعد التي لا يكون فيها الشاهد حاضرا جسديا وإنما تتم عبر وسائل إلكترونية أو رقمية من خلال شبكة الإنترنت، كما قد تكون هذه الشهادة مسجلة مسبقا أو تكون فورية[7].

---

[1] القسم الرابع من الفصل الأول من الباب الثالث تحت عنوان: سماع الشهود المواد: (99-88) من (ق.إ.ج.ج)، والتي تتلخص حول استدعاء الشهود وحضورهم وكيفية تلقي إفاداتهم وحلف اليمين والحالات التي لا يجوز فيها سماع الشخص كشاهد ونصاب الشهادة...إلخ.

[2] علي عدنان الفيل، المرجع السابق، ص61.

[3] هبة حسين محمد زايد، المرجع السابق، ص209.

[4] عبد الرحمان خلفي، المرجع السابق، ص175.

[5] محمد حزيط، المرجع السابق، ص110.

[6] عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق، ص21، راجع أيضا، فؤاد حسن العزيزي المرجع السابق، ص198.

[7] تتلخص أنواع الشهادة في:

- الشهادة الشفهية والشهادة المكتوبة : في الغالب يتم الإدلاء بالشهادة بالتصريح الشفوي بحيث يصرح الشهود شخصيا للقاضي عما رأوه أو ما سمعوه، وكاستثناء عن هذه القاعدة يمكن أن تتم الشهادة بطريق الكتابة كالأوراق الإعترافية أو في الرسائل، وزيادة على ذلك فإن الوسائل السمعية البصرية الحديثة قد أظهرت نوعا آخرا من الشهادة تتمثل في التسجيلات والأشرطة ...إلخ.==

في هذا المجال تنبه المشرع الجزائري إلى أهمية استعمال وسائل تكنولوجيا المعلومات في عصرنة العدالة بقصد تسهيل إجراءات التقاضي، ومنها قبول الشهادة عن بعد، حيث انطلقت بمحكمة القليعة بالجزائر العاصمة في شهر أكتوبر 2015، أول محاكمة مرئية عن بعد "اختيارية" دون نقل المتهم إلى قاعة الجلسات في خطوة تُعد سابقة في تاريخ العدالة الجزائرية. كما يهدف هذا الإجراء إلى القضاء على الاكتظاظ بالمحاكم، وتخفيف عناء التنقل، وتسهيل عملية المحاكمة، وكذا تخفيف الضغط على الأسلاك الأمنية وإدارة السجون المكلفة بنقل المتهمين وتقليص المسافات على الشهود الموجودين في أماكن بعيدة عن مجريات المحاكمة[1].

ثانيا: مفهوم الشاهد المعلوماتي: تُعد شهادة الشهود في الجرائم الإلكترونية من الأدلة الهامة التي يمكن تقديمها للمحكمة، لكونها عاملا حاسما يمثل منطق التعامل مع الطبيعة الخاصة لهذه الجرائم المستحدثة، فالشاهد في الجريمة الإلكترونية هو ذلك:" الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي، وذلك تمييزا له عن الشاهد التقليدي"[2] ويشمل الشاهد المعلوماتي بهذا المفهوم عدة أقسام أهمها[3]:

== – الشهادة المباشرة والشهادة غير المباشرة : الشهادة المباشرة وهي الأصل حيث يخبر الشاهد عما رآه بعينه أو سمعه بأذنه. أما الشهادة غير المباشرة أو السماعية فهي أن يشهد الشاهد على الواقعة محل الإثبات بما سمعه عن آخر يكون قد رآها بعينه أو سمعها بأذنه.

- الشهادة بالتسامع: تختلف الشهادة بالتسامع عن الشهادة السماعية المتعلقة بأمر معين نقلا عن شخص معين شاهدا هذا الأمر بنفسه كما تتعلق الشهادة بالتسامع بأمر معين، لكنها ليست نقلا عن شخص معين شاهد الأمر بنفسه، فيقول الشاهد سمعت كذا أو أن الناس قالوا كذا دون أن يستطيع إسنادها لأشخاص معينين، راجع، خالد ممدوح إبراهيم، فن التحقيق، المرجع السابق، ص ص259-260 وأيضا عمر محمد أبو بكر بن يونس، الرسالة السابقة، ص ص954-955.

[1] تندرج العملية في إطار مواصلة العدالة الجزائرية لعصرنة القطاع من خلال استعمال تكنولوجيات الإعلام والاتصال في القطاع على "أمل تحقيق العدالة الإلكترونية" .وقد تم إجراء المحاكمة علنية بحضور هيئة الدفاع ومفتوحة للمواطنين بإحدى قاعات الجلسات فيما خصصت قاعة مجهزة بالوسائل السمعية البصرية بالمؤسسة العقابية بالقليعة تعمل بالألياف البصرية وفق نظام الشبكة الداخلية لوزارة العدل. حيث امتثل فيها ثلاثة متهمين في ثلاث جنح، خضعوا لمحاكمة علنية عادية، دون الحاجة إلى نقلهم خارج أسوار السجن، راجع إجراء أول محاكمة قضائية مرئية عن بعد بمحكمة القليعة، خبر منشور على الموقع الرسمي للإذاعة الجزائرية: *http://www.radioalgerie.dz/news/ar/article/20151008/54527.html*،تاريخ الاطلاع:2016/04/02 على الساعة:10:09.

[2] خالد ممدوح ابراهيم، فن التحقيق، المرجع السابق، ص263.

[3] عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص ص612-613، راجع أيضا، عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق، ص21.

1- **القائم على تشغيل الحاسوب:** وهو المسؤول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به، ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات، كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج ..إلخ.

2- **المبرمجون** :وهم الأشخاص المتخصّصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين: الفئة الأولى: هم مخططو برامج التطبيقات الذين يتولون اختيار وتعديل برامج نظام الحاسب الداخلية لتجهيز الحاسوب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والاخراج، ووسائط التخزين بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج. أما الفئة الثانية: هم مخططو برامج النظم، الذين يقومون بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات.

3- **المحللون:** المحلل وهو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات.

4- **مهندسو الصيانة والاتصالات:**وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

5- **مديرو النظم:**وهم الذين يُوكل لهم أعمال الإدارة في النظم المعلوماتية.

تطبيقا لمفهوم الشاهد المعلوماتي وبالرجوع إلى نص المادة 05 الفقرة الأخيرة من القانون رقم: 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أجاز المشرع الجزائري للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها، فقد يطلب هذا الشخص على سبيل مساعدة السلطات القضائية في جوانب تقنية لحل لغز الجريمة، كما قد يستعين به الخبير في انجاز الخبرة الرقمية بموافقة سلطات التحقيق، كما يمكن أيضا أن يحمل صفة الشاهد المعلوماتي في جريمة وقعت في المؤسسة التي يعمل بها. ومثال ذلك طلب الجهات القضائية من مهندس في الإعلام الآلي تخصّص برمجة شهادته للكشف عن ملابسات الجريمة.

كما نص أيضا بموجب المادة (10) من القانون نفسه التي تحدد التزامات مقدمي الخدمات والتي من بينها مساعدة السلطات القضائية المكلفة بالتحريات لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات وكذلك حفظ المعطيات المتعلقة بحركة السير[1]، والأمر نفسه نصت عليه المادة

---

[1] المادتان (11-10) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(12) من القانون نفسه حينما نصت على الالتزامات الخاصة لمقدمي خدمة الإنترنت مثل: حفظ المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال وكذا المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم للاتصال وكذا عناوين المواقع المطلع عليها...إلخ[1]. ففي كل هذه الحالات يمكن للجهات القضائية طلب تدخل هؤلاء الأشخاص سواء كانوا أشخاصا طبيعيين أو معنويين بصفتهم كشهود معلوماتيين، إذا تطلبت مقتضيات التحقيق ذلك.

الفرع الثاني: التزامات الشاهد المعلوماتي:

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله، لكن بالمقابل يُثار التساؤل: هل أن الشاهد المعلوماتي ملزم بطبع ملفات البيانات المخزنة في ذاكرة الحاسوب؟ أو هل يجوز له الإفصاح عن كلمات المرور السرية والشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج؟. في هذا الصدد برز هناك اتجاهان نتطرق إليهما كما يأتي:

– **الاتجاه الأول:** يرى أصحاب هذا الاتجاه، أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة، أن يقوم بطبع ملف البيانات أو الافصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة. ويميل إلى هذا الاتجاه الفقه الألماني، حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بإدلاء الشهادة لا يتضمن هذا الواجب، وفي تركيا لا يجوز حمل الشاهد على الإفصاح عن كلمات المرور السرّية أو كشف شفرات تشغيل البرامج المختلفة[2].

– **الاتجاه الثاني:** يرى أنصار هذا الاتجاه أن من بين الالتزامات التي تقع على عاتق الشاهد المعلوماتي، القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة. حيث يرى اتجاه في الفقه الفرنسي أن القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية، ومن ثمة يتعين على الشهود من حيث المبدإ الإلزام بتقديم شهادتهم ومن ثم يجب عليهم الافصاح عن كلمات المرور السرية التي يعلمونها، ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا في مرحلة التحقيق والمحاكمة. كما يجيز المشرع الهولندي بموجب قانون الحاسب الآلي لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل النظام لتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله كالإفصاح عن كلمات المرور السرّية والشفرات الخاصة بتشغيل البرامج المختلفة، وإذا وجدت بيانات مشفرة أو مرمزة داخل ذاكرة الحاسب وكانت

---

[1] المرجع نفسه، المادة (12).

[2] علي عدنان الفيل، المرجع السابق، ص64.

مصلحة التحقيق تستلزم الحصول عليها، يتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات[1].

إن طبيعة التحقيق في الجرائم الإلكترونية توجب على الشاهد المعلوماتي الإدلاء إلى القضاء بكل ما يحوزه من معلومات جوهرية مثل: شيفرات الدخول للنظام المعلوماتي لاستخراج الأدلة الرقمية...إلخ. وقد وضع المشرع الجزائري أمام الشاهد بصفة عامة كل الوسائل التي تمكنه من الإدلاء بشهادته دون زيادة أو نقصان وتحت طائلة العقوبات في حالة عدم الحضور أو رفضه للشهادة بعد تصريحه بمعرفة الجاني[2]. غير أن التنظيم القانوني للقواعد الإجرائية في الدعاوى المعتمدة على أدلة رقمية والتي تتصل أساسا بالعالم الافتراضي يجب إعادة توصيفها قانونا، بل وتنظيمها بشكل لا يضع الشاهد موضع المساءلة في حالة إخلاله بالسر المهني بما لا يحرم القضاء فرصة الإفادة من شهادة الشاهد في الكشف عن الجريمة الإلكترونية، خاصة في ظل صعوبة استخلاص الأدلة الرقمية في هذا النوع من الجرائم[3].

وعموما هناك شروطا يجب توافرها لإلزام الشاهد المعلوماتي بالإعلام في الجرائم الإلكترونية وهي:

-**الشرط الأول: وقوع جريمة إلكترونية:** حتي يلتزم الشاهد المعلوماتي بالإعلام في الجريمة الإلكترونية، لابد أن تكون هذه الجريمة قد وقعت بالفعل، كما لا يكفي وقوع أية جريمة، بل لابد من وقوع جناية أو جنحة أما المخالفات فهي تستبعد لأنها هيّنة الأثر[4].

-**الشرط الثاني: علم الشاهد المعلوماتي بالمعلومات الجوهرية المتصلة بالواقعة:** يعتبر علم الشاهد بمضمون النظام المعلوماتي محل الواقعة الجرمية شرطا هاما في إلزامه بالشهادة مثل: طبع الملفات الخاصة بالبيانات والإفصاح عن كلمات السر والكشف عن مفاتيح الشفرات...إلخ[5].

-**الشرط الثالث: أن تقتضي مصلحة التحقيق هذه الشهادة:** لإلزام الشاهد الإدلاء بالمعلومات الجوهرية لا بد أن تتطلب مصلحة التحقيق ذلك، خاصة إذا تطلب الأمر اختراق النظام المعلوماتي بقصد البحث عن الدليل الرقمي[1].

---

[1] المرجع نفسه، ص ص 64-65.

[2] حيث تنص المادة (98) من (ق.إ.ج.ج) على: "كل شخص بعد تصريحه علانية بأنه يعرف مرتكبي جناية أو جنحة يرفض الإجابة على الأسئلة التي توجه إليه في هذا الشأن بمعرفة قاضي التحقيق يجوز إحالته إلى المحكمة المختصة والحكم عليه بالحبس من شهر إلى سنة وبغرامة من 1.000 إلى 10.000 دينار أو بإحدى هاتين العقوبتين".

[3] هبة حسين محمد زايد، المرجع السابق، ص223.

[4] عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص623.

[5] هبة حسين محمد زايد، المرجع السابق، ص226.

المطلب الرابع: حالة التلبّس في الجريمة الإلكترونية

علاوة على الاختصاصات العادية للضبطية القضائية، نص المشرع الجزائري على بعض الاختصاصات الاستثنائية والمتعلقة بالجرائم المتلبّس بها، أو كما تسمى أيضا "بالجريمة المشهودة" والهدف من وراء ذلك هو المحافظة على أدلة إثبات الجريمة من الضياع وحتى لا يعبث بها المجرم. سنتناول مفهوم التلبس وحالاته واختصاصات الضبطية القضائية في (الفرع الأول)، ثم نتطرق إلى مدى تحقّق حالات التلبس في مجال الجريمة الإلكترونية في (الفرع الثاني).

الفرع الأول: مفهوم التلبّس، حالاته، واختصاصات الضبطية القضائية فيه:

تتمتع الجريمة المتلبس بها بماهية تختلف عن باقي الجرائم.

– **أولا: تعريف التلبّس:** لم يتطرق المشرع الجزائري إلى تعريف التلبّس، وإنما تطرق إلى حالات التلبس بالجريمة المحددة على سبيل الحصر وفق نص المادة (41) (ق.إ.ج.ج)، والتي سنتطرق إليها لاحقا، وبالرجوع إلى الفقه فالتلبّس عبارة عن وصف عيني للجريمة وليس بوصف شخصي، فالجريمة هي التي تكون متلبس بها ومشهودة وليس فاعلها. وعليه يعتبر التلبّس وصفا خاصا بالجريمة يفيد معنى التقارب الزمني بين وقوع الجريمة وكشفها[(2)].

وعليه تتعلق حالة التلبّس باكتشاف الجريمة في وقت معين، ولا تتعلق بأركان الجريمة أو مراحل تنفيذها. ويتميز التلبّس بأنه مرتبط بالجريمة دون فاعلها وتكون الجريمة في حالة تلبّس بسماع صوت استغاثة المجني عليه إثر سماع صوت طلقات الرصاص مثلا، ولو لم يشاهد من أطلقه، وفي حالة شم رائحة مخدر تتصاعد من مسكن المتهم، ولو لم يشاهد أثناء تدخينه إياه، وفي حالة رؤية حريق مشتعل رغم عدم وجود الجاني، وحتى إذا شُوهد المذكور أثناء ارتكابه للجريمة فلا يكون متلبّسا بالجريمة، وإنما الجريمة هي التي تكون في حالة تلبس.

كما يستلزم التلبس ذو الآثار الإجرائية المتميزة وجود مظاهر خارجية تنبئ بذاتها عن ارتكاب الجريمة، إما بمشاهدة الركن المادي للجريمة وقت مباشرته، أو برؤية ما يكشف عن وقوعها منذ فترة وجيزة. فلا يكفي مثلا أن يشاهد ضابط الشرطة القضائية المتهمة المعروفة باعتيادها ممارسة الدعارة تدخل بإحدى الشقق للقول بأن جريمة الاعتياد على ممارسة الدعارة تعتبر في حالة تلبس، إذ أن هذا الدخول لا ينبئ بذاته عن إدراك الضابط بطريقة يقينية ارتكاب تلك الجريمة. ومن باب أولى فإن الأدلة القولية على وقوع الجريمة لا تقوم بها حالة تلبس، في حالة علم ضابط الشرطة القضائية

---

[1] خالد ممدوح إبراهيم، فن التحقيق، المرجع السابق، ص265.

[2] عبد الرحمن خلفي، المرجع السابق، ص57.

للجريمة عن طريق أحد أعوانه، إذ يجب أن يدرك هو ذاته المظاهر الخارجية، كي يباشر السلطات التي يخوله القانون إياها[1].

ثانيا: حالات التلبّس: تنص المادة (41) من (ق.إ.ج.ج) على:" توصف الجناية أو الجنحة بأنها في حالة تلبّس إذا كانت مرتكبة في الحال أو عقب ارتكابها. كما تعتبر الجناية أو الجنحة متلبّسا بها إذا كان الشخص المشتبه في ارتكابه إياها في وقت قريب جدا من وقت وقوع الجريمة قد تبعه العامة بصياح أو وجدت في حيازته أشياء أو وجدت آثار أو دلائل تدعو إلى افتراض مساهمته في الجناية أو الجنحة. وتتسم بصفة التلبس كل جناية أو جنحة وقعت ولو في غير الظروف المنصوص عليها في الفقرتين السابقتين، إذا كانت قد ارتكبت في منزل أو كشف صاحب المنزل عنها عقب وقوعها وبادر في الحال باستدعاء أحد ضباط الشرطة القضائية لإثباتها."

من خلال نص المادة نستنتج حالات التلبّس التي أوردها المشرع الجزائري على سبيل الحصر وهي:

الحالة الأولى: مشاهدة الجريمة حال ارتكابها: والتي يعبر عنها بالتلبّس الحقيقي وهنا يتم رؤية الجريمة أثناء ارتكابها، ولفظ المشاهدة ينصرف إلى جميع الحواس كالرؤية والسمع والشم والتذوق واللّمس...إلخ. كما قد تكون المشاهدة من طرف ضابط الشرطة القضائية سواء كانت بصورة مباشرة أو بعد الانتقال إلى مسرح الجريمة بعد الإبلاغ عنها قصد معاينة آثارها، ومنه تعد ضمن حالات التلبّس عندما يشم ضابط الشرطة القضائية رائحة المخدرات في مكان يوجد به من يستعملها[2].

الحالة الثانية: مشاهدة الجريمة عقب ارتكابها: هنا لا يتم مشاهدة الجريمة حال ارتكابها، بل تكون المشاهدة بعد مدة زمنية قصيرة من ارتكابها، ولم يحدد المشرع الجزائري المدة الزمنية واكتفى بأن عبّر عنها بعبارة "عقب ارتكابها"، وعليه نفهم هنا بأن المدة الزمنية يجب أن تكون قصيرة وتخضع في تقديرها لقضاة الموضوع[3].

الحالة الثالثة: متابعة العامة للمشتبه فيه بالصياح: في هذه الحالة لا تعتمد على المشاهدة وإنما تعتمد على عنصر المتابعة المادية للمشتبه فيه من طرف العامة مرفقة بالصياح. ويجب التفريق بين صياح العامة والإشاعة العامة التي لا تتعدى أن تكون إلا مجرد أقاويل متداولة بين الناس، في حين أن الصياح يكون بالصراخ، وهو عبارة عن اتهام مباشر للجاني من قبل الناس الذين شهدوا وقوع

---

[1] عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص ص442-443.

[2] حسين طاهري، الوجيز في شرح قانون الإجراءات الجزائية، دار المحمدية العامة، الجزائر، ط2، 1999، ص ص33-34، راجع أيضا، عبد الرحمن خلفي، المرجع السابق، ص59.

[3] محمد حزيط، المرجع السابق، ص63.

الجريمة للمساعدة في إلقاء القبض على الفاعل دون اشتراط أن يتم القبض عليه فعلا[1]. كما لم يحدد المشرع الجزائري المدة الزمنية الفاصلة بين صياح العامة ومشاهدتهم للفعل المجرم، بل اكتفى بالنص على ذلك بعبارة "في وقت قريب جدا" من ارتكابها، وعليه يُفهم هنا بأنه يجب أن يُعقب تنفيذ الركن المادي للجريمة وقتا قصيرا، وتبقى مسألة تحديده للسلطة التقديرية لضابط الشرطة القضائية تحت مراقبة قاضي الموضوع.

الحالة الرابعة: ضبط أداة الجريمة بحوزة المشتبه فيه: كأن يتم ضبط سلاح أو مسروقات بحوزته تدل على ارتكابه الفعل المجرم أو مشاركته فيه، بحيث تعد قرينة قوية ضد المشتبه فيه، غير أنه يشترط أن تكون هناك صلة وثيقة بين وجود هذه الأشياء مع المتهم، وبين حادث الجريمة كما تكون في وقت قريب جدا من ارتكابها[2].

الحالة الخامسة: وجود آثار أو دلائل تفيد ارتكاب الجريمة: تدخل ضمن حالات التلبّس وُجود خُدوش أو جُروح أو بُقع دم أو قُصاصات من شعر المجني عليه على جسم المشتبه فيه، كما لم يحدد المشرع الفاصل الزمني بين وقوع الجريمة ومشاهدة الجاني واستعمل "في وقت قريب جدا" تاركا تقدير هذا الفاصل الزمني لقضاة الموضوع[3].

الحالة السادسة: اكتشاف جريمة في مسكن والتبليغ عنها في الحال: يقصد بهذه الحالة أن ترتكب الجناية أو الجنحة في منزل، حيث يكتشف صاحبه هذه الجريمة في وقت غير معلوم لديه ويبادر في الحال إلى إبلاغ ضابط الشرطة القضائية، ثم يقوم هذا الأخير بالانتقال فورا إلى المنزل ودون تمهّل لمعاينة الجريمة بعد إبلاغ وكيل الجمهورية [4] مثل اكتشاف الزوج زوجته متلبّسة بجريمة الزنا.

حتى يكون التلبس صحيحا ومنتجا لآثاره القانونية خاصة ما تعلق بممارسة الاختصاصات الاستثنائية لضباط الشرطة القضائية، لابد من توافر جملة من الشروط تتمثل أساسا في[5]:

- أن يكون التلبّس سابقا على الإجراء.

---

1 عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص452.

2 عبد الرحمن خلفي، المرجع السابق، ص60.

3 محمد حزيط، المرجع السابق، ص63.

4 حيث تنص المادة (42) من (ق.إ.ج.ج) على:" يجب على ضابط الشرطة القضائية الذي بلّغ بجناية في حالة تلبّس أن يُخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهّل إلى مكان الجناية ويتخذ جميع التحريات اللاّزمة...".

5 عبد الرحمن خلفي، المرجع السابق، ص61، راجع أيضا، عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص460.

- مشاهدة التلبّس بمعرفة ضابط الشرطة القضائية وإن بلّغ عنه، يجب عليه الانتقال فورا لمعاينته.
- يجب أن يتم اكتشاف التلبّس بطريق مشروع.

ثالثا: اختصاصات الضبطية القضائية في حالات التلبس: إذا توافرت إحدى حالات التلبّس بموجب المادة (41) من (ق.إ.ج.ج)، رتّب القانون لضباط الشرطة القضائية آثارا منها ما تعلق بسلطات الاستدلال، ومنها ما تعلق بسلطات التحقيق المتعلقة بحالة التلبّس.

1- سلطات الاستدلال المترتبة على التلبس: حيث تنص المادة (42) من (ق.إ.ج.ج) على:" يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية ويتخذ جميع التحريات اللازمة. وعليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي. وأن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة. وأن يعرض الأشياء المضبوطة على الأشخاص المشتبه في مساهمتهم في الجناية للتعرف عليها". وعليه تتلخص سلطات الاستدلال فيما يأتي[1]:

- يجب إخطار وكيل الجمهورية حالا والانتقال لمكان الجريمة دون تمهل.
- يجب أن يعاين الآثار المادية للجريمة ويُحافظ عليها.
- ضبط كل ما يفيد في كشف الحقيقة (سلاح، ملابس، أوراق، صُور...إلخ).
- عرض الأشياء المضبوطة على الأشخاص المشتبه في مساهمتهم في الجناية قصد التعرف عليها بما يفيد في كشف الجريمة.

2- سلطات التحقيق المترتبة على التلبس: إن الأصل في هذه الإجراءات هي من اختصاص قاضي التحقيق، لكن خوّلها المشرع استثناء لضباط الشرطة القضائية في حالة التلبس لاعتبارات عملية تتعلق بالخوف من ضياع آثار الجريمة، نذكر بعضها في ما يأتي:

- الأمر بعدم المبارحة أو عدم المغادرة : عدم المبارحة أمر يوجهه ضابط الشرطة القضائية المتواجد في مكان ارتكاب الجريمة للمعاينة لشخص أو لعدة أشخاص يتواجدون بمكان الجريمة والهدف من ذلك التعرف على هوية الشخص وسماع أقوال من يكون قد حضر الجريمة، وجمع المعلومات بشأن الجريمة المتلبس بها. غير أنه في حالة عدم الامتثال لأمر الضابط يقوم هذا الأخير

[1] عبد الرحمن خلفي، المرجع السابق، ص62.

بتحرير محضر بالمخالفة المرتكبة ويقدمه للسلطة المختصة لتوقيع الجزاء وفقا لنص المادة (50) من(ق.إ.ج.ج) والغرض من ذلك إتمام مهمته على أحسن وجه[1].

– ضبط المشتبه فيه واقتياده إلى مركز الشرطة : الضبط هو التعرض المادي للشخص بتقييد حريته واقتياده إلى أقرب مركز شرطة أو الدرك، يجوز أن يقوم به عامة الناس أو رجال الشرطة بشرط وجود حالة التلبّس[2] .

– الاستعانة بالخبراء: يمكن لضباط الشرطة القضائية في المعاينات التي لا يمكن تأخيرها الاستعانة بأشخاص مؤهلين، كما لم يحدد المشرع نوع المهمة التي يقومون بها، إلا أنها تهدف إلى إظهار الحقيقة[3].

رأينا سلفا حالات التلبّس واختصاصات الضبطية القضائية بخصوص الجرائم التقليدية، لكن بالمقابل يُثار التساؤل حول مدى صلاحية صور التلبّس للجرائم الإلكترونية؟ هذا ما سنتطرق إليه في الفرع الموالي.

الفرع الثاني: مدى تحقّق حالات التلبس في مجال الجريمة الإلكترونية:

يرى البعض أنه من الممكن تطبيق صور الجريمة المتلبس بها في نطاق الجرائم الإلكترونية وذلك في حال اكتشاف ضابط الشرطة القضائية أو المجني عليه الجاني أثناء قيامه باختراق شبكة معينة أو نظام معلوماتي أو قاعدة بيانات، بشرط وجود الإمكانات الفنية لتتبع ومطاردة الجاني للتعرف عليه[4]. كما يمكن مشاهدة الجريمة وقت حدوثها عبر شبكة الإنترنت عن طريق وسائل التواصل الاجتماعي سواء من طرف ضابط الشرطة القضائية مباشرة أو حينما يتم إبلاغه بذلك، وهذا ما وقع فعلا في الولايات المتحدة الأمريكية في سنة 2011 [5]. ففي هذه الصورة تتحقق حالة من

---

[1] حيث تنص المادة (50) من (ق.أ.ج.ج) على:" يجوز لضابط الشرطة القضائية منع أي شخص من مبارحة مكان الجريمة ريثما ينتهي من إجراء تحرياته. وعلى كل شخص يبدو له ضروريا في مجرى استدلالاته القضائية التعرف على هويته أو التحقق من شخصيته أن يمتثل له في كل ما يطلبه من إجراءات في هذا الخصوص. وكل من خالف أحكام الفقرة السابقة يعاقب بالحبس مدة لا تتجاوز عشرة أيام وبغرامة 500 دينار".

[2] حيث تنص المادة (61) من (ق.إ.ج.ج) على:" يحق لكل شخص في حالات الجناية أو الجنحة المتلبس بها والمعاقب عليها بعقوبة الحبس، ضبط الفاعل واقتياده إلى أقرب ضابط للشرطة القضائية".

[3] حيث تنص المادة (49) من (ق،إ.ج.ج) على:" إذا اقتضى الأمر إجراء معاينات لا يمكن تأخيرها فلضابط الشرطة القضائية أن يستعين بأشخاص مؤهلين لذلك. وعلى هؤلاء الأشخاص الذين يستدعيهم لهذا الإجراء أن يحلفوا اليمين كتابة على إبداء رأيهم بما يمليه عليهم الشرف والضمير."

[4] فايز محمد راجح غلاب، الأطروحة السابقة، ص288.

[5] تعود وقائع القضية إلى قيام شخص لم يكشف عن هويته بإبلاغ الشرطة الأميركية بجريمة قتل وقعت خلال "دردشة" له مع امرأة بالفيديو عبر الإنترنت. حيث ذكرت إحدى الصحف الأمريكية أن الشخص شاهد جريمة قتل (ميليني هاين) (31سنة) من منطقة ليبانون بولاية بنسيلفانيا خلال محادثته معها على الإنترنت، حيث أطلق زوجها (سكوت هاين) (33 سنة) النار عليها من مسدسه وأرداها قتيلة.

حالات التلبّس وهي المشاهدة عن بعد وعبر موجات كهرومغناطيسية مثل ما تتحقق المشاهدة المادية الملموسة في الجريمة التقليدية.

كما يمكن أيضا أن تتحقق صورة مشاهدة الشخص للجاني بعد ارتكابه للجريمة في الحال أو عقب ارتكابها، ومثال ذلك أن يقوم صاحب محل الإنترنت أثناء مراجعته للحاسوب عقب استخدامه من طرف العميل وقبل مغادرته للمحل، باكتشاف ملفات تثير الاشتباه وعند فتحها تبين أنها تحتوي على صور دعارة تم تنزيلها أثناء إبحار العميل في شبكة الإنترنت مما يسمح بقيام حالة التلبس، ولكن بشرط قبل مغادرة العميل لمحل الإنترنت. كما تُعد أيضا مراقبة حركات العميل المشكوك فيها بمحاولة اختراق أجهزة حاسوب الغير أو الأنظمة المعلوماتية واكتشاف ذلك من قبيل حالة التلبس[1]. وبرغم تصور وجود تطابق في حالات التلبّس بين الجريمة التقليدية والجريمة الإلكترونية، إلا أن الصياح في الجريمة الإلكترونية غير متصور حدوثه، بسبب حدوث التتبع في عالم افتراضي، ومع ذلك هناك من الآراء من لا يشترط أثناء التتبع وقوع الصياح مثل: أن يكون المجني عليه أخرص أو لا يستطيع الصياح لأي سبب معين إذا تكفي الإشارة بالأيدي[2].

كما رأينا سلفا أن من شروط صحة التلبّس أن يتم اكتشافه بطريق مشروع، لذا تثار في هذه المسألة مشكلة مشروعية التخفي عبر الإنترنت من طرف المكلف بالتحريات قصد الكشف عن الجريمة الإلكترونية ومرتكبيها، وذلك باستعمال أسماء وهمية ومن ثمة الدخول إلى غرف المحادثات وحلقات النقاش. غير أن المشرع الجزائري عالج هذه المشكلة تحت مصطلح التسرّب بدلا من مصطلح التخفي، وهذا بموجب الفصل الخامس تحت عنوان: "في التسرّب" المواد (65 مكرر11 – 65 مكرر18) من (ق.إ.ج.ج)، وهو إجراء جديد يُضاف إلى الإجراءات التقليدية مما يمكّن أجهزة البحث والتحري من الكشف عن المجرم الإلكتروني في هذه البيئة الافتراضية التي يصعب التحقيق فيها بسبب طبيعتها الخاصة. فإذا شاهد ضابط الشرطة القضائية المكلف بعملية التسرّب جريمة متلبّس بها، عليه القيام بالإجراءات الاستثنائية المخولة له قانونا لأنه يوجد في حالة مشروعة.

من جهة أخرى تثار مشكلة حساب الوقت اللاّزم لقيام حالة التلبّس في الجريمة التقليدية فاستعمل المشرع الجزائري مصطلحات "مرتكبة في الحال أو عقب ارتكابها" و" في وقت قريب جدا من وقت الجريمة"، وهذا أمر يترك تحديده لضابط الشرطة القضائية ولقاضي الموضوع تقدير

وبعد الحادثة صعد الزوج القاتل إلى غرفة النوم في المنزل وانتحر بإطلاق النار على نفسه، نُشرت تفاصيل هذه القضية على مواقع عديدة منها *http://www.al-jordan.com/?p=1104*، تاريخ الاطلاع:2016/08/04 على الساعة:07:00.

[1] عمر محمد أبوبكر بن يونس، الرسالة السابقة، ص848.

[2] فايز محمد راجح غلاب، الأطروحة السابقة ، ص ص289-290.

المسألة، بخلاف تقدير الزمن اللاّزم في الجريمة الإلكترونية، والتي يصعب تحديده لاسيما إذا كانت هناك ملاحقة بسبب الطبيعة الخاصة لهذه الجريمة.

تناولنا سلفا الإجراءات الاستثنائية لضباط الشرطة القضائية بخصوص الجريمة المتلبس بها ومنها تفتيش منزل المتهم وكذا حاسوبه، إذ يتطلب ذلك وجود إذن قضائي وهذا بموجب المادة(44) من (ق.ا.ج.ج) التي تنص على:" لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء متعلقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش. ويكون الأمر كذلك في حالة التحري في الجنحة المتلبّس بها أو التحقيق في إحدى الجرائم المذكورة في المادتين 37 و40 من هذا القانون..." وعليه لا يتم إجراء التفتيش إلا بناء على إذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا الأمر قبل الدخول إلى المنزل. ويكون الأمر كذلك في حالة التحري عن الجنح المتلبّس بها أو التحقيق في بعض الجرائم، ومنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

بالنظر للطبيعة الخاصة للجرائم الإلكترونية، يتعارض هذا مع حالة الاستعجال التي تتطلب السرعة في اتخاذ الإجراءات الكفيلة بالحفاظ على الأدلة في مجال الإجرام الإلكتروني، لأن استصدار إذن قضائي يتطلب وقتا قد يكون طويلا بما يفوّت الفرصة على ضابط الشرطة القضائية للإمساك بكافة خيوط الجريمة. في هذا الشأن خالف المشرع الجزائري نظيره الفرنسي الذي ينص في المادة (56) من (ق.إ.ج.ف)على جواز التفتيش في حالة التلبّس دون إذن قضائي في الجناية التي يمكن إثباتها عن طريق حجز أوراق أو مستندات، أو معطيات معلوماتية، أو أشياء تتعلق بالجريمة، فيمكن لضابط الشرطة القضائية التنقل إلى منزل المتهم وتفتيشه وتحرير محضر بذلك[1].

بناء على ما سبق يتضح لنا: أن المشرع الجزائري أجاز تفتيش منزل المتهم وحاسوبه في الجرائم المتلبس بها من خلال النص على ذلك بموجب المادة (44) سالفة الذكر، ومنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات بشرط وجود إذن من وكيل الجمهورية أو قاضي التحقيق

---

[1] ***Article 56 du (CPPF) :***

"Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal..." .

كما أنه من جهة أخرى نص على قواعد تفتيش المنظومة المعلوماتية وحجز المعطيات –والذي سنتطرق إليه لاحقا–في إطار تطبيق قانون الإجراءات الجزائية وهذا بموجب المواد من (09–05) من القانون رقم: 09–04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وعليه نلاحظ أن صور الجريمة المتلبّس بها المنصوص عليها بموجب المادة (41) من (ق.إ.ج.ج) غير كافية لاستيعاب كافة أشكال الجرائم الإلكترونية المتلبّس بها، بسبب أن هذه النص وُضع لمعالجة الجريمة التقليدية التي تتم في وسط مادي بعكس الجريمة الإلكترونية التي ترتكب في بيئة افتراضية، خاصة عندما اشترط المشرع وجود إذن التفتيش حتى في الجريمة المتلبّس بها ومنها الجريمة الإلكترونية.

بالرجوع إلى الأنظمة القانونية الإجرائية الحالية، يلاحظ أن هناك قصورا بخصوص أساليب البحث والتحري التقليدية في استخلاص الدليل الرقمي للكشف عن الجرائم الإلكترونية وملاحقة مرتكبيها. فالمشرع أجاز استخلاص الدليل عموما وفق ضوابط إجرائية معينة منها: الانتقال والمعاينة الخبرة، التفتيش وضبط الأدلة، الشهادة...إلخ، كما أن هذه الإجراءات تخص استخلاص الدليل من الجرائم سواء كانت تقليدية أم مستحدثة، والأكيد أن إجراءات جمع الدليل الرقمي في هذه الجرائم غير كافية لاستيعاب كافة أشكال الجريمة الإلكترونية، فهي تحتاج من المشرع تعديلها أو استحداث أخرى جديدة لمواكبة التطورات التقنية المتلاحقة في مجال مكافحة الجريمة الإلكترونية. وهذا ما قام به المشرع فعلا لاستدراك هذا النقص، حيث استحدث في سياسته الجنائية الإجرائية مجموعة أساليب جديدة للبحث والتحري عن الجرائم المستحدثة ومنها الجرائم الإلكترونية، وهذا ما سنتطرق إليه في المبحث الموالي.

المبحث الثاني: أساليب البحث والتحري المستحدثة في الكشف عن الجرائم الإلكترونية

خلصنا في المبحث السابق إلى عدم كفاية وفعالية الإجراءات التقليدية المتعلقة بالبحث والتحري عن الجرائم الإلكترونية، والتي ترمي إلى جمع الدليل الإلكتروني لإدانة المجرم المعلوماتي نظرا لاعتماد هذا الأخير على تقنية المعلومات الحديثة. لذا أصبح من الضروري اعتماد المشرع على وسائل حديثة لكشف الجريمة والقبض على مرتكبيها وعدم إفلات المجرم من العقاب ضمن هذا النوع المستحدث من الجرائم، وعليه قام المشرع الجزائري بتعديلات متتالية لأحكام قانون الإجراءات الجزائية بهدف جعله يتطابق مع ما جاء في المواثيق والاتفاقيات الدولية في هذا المجال، وذلك بإدراج قواعد إجرائية جديدة تتمثل في أساليب وآليات حديثة تتلائم وطبيعة هذه الجرائم وهذا بموجب المادة(65 مكرر05 – 65 مكرر10) من القانون رقم:06–22 المؤرخ في:2006/12/22 يعدل ويتمم قانون الإجراءات الجزائية. وفي الوقت نفسه أحاطها بجملة من الضمانات بهدف عدم المساس بحرمة الحياة

الخاصة للأفراد المكفولة دستوريا. ونظرا لارتباط هذه الإجراءات المستحدثة بحرمة الحياة الخاصة للأفراد، وما يمكن أن يشكّله ذلك من خطر عليها، سنقوم بتوضيح الاختصاص القضائي لكل جهة قضائية بخصوص البحث والتحري عن الجرائم الإلكترونية.

وعليه ارتأينا تقسيم هذا المبحث إلى أربعة مطالب، نتناول اعتراض المراسلات وتسجيل الأصوات في (المطلب الأول)، ثم نتطرق بعدها إلى التقاط الصور في (المطلب الثاني)، لنتعرف على إجراء التسرّب في (المطلب الثالث)، لنختم في الأخير بالحديث عن الاختصاص القضائي بخصوص البحث والتحري عن الجرائم الإلكترونية لكل من وكيل الجمهورية وقاضي التحقيق إضافة إلى الصلاحيات المكانية للضبطية القضائية في (المطلب الرابع).

المطلب الأول: في مجال اعتراض المراسلات وتسجيل الأصوات

تعتبر هذه الإجراءات المستحدثة مكسبا هاما لسلطات البحث والتحري في الكشف عن بعض الجرائم المحددة على سبيل الحصر ومنها الجرائم الإلكترونية، وهذا برغم ما قد يشكله من مساس بحرمة الحياة الخاصة المكفولة قانونا، إذا لم تتم وفق الشروط القانونية المطلوبة. سنتناول مفهوم اعتراض المراسلات وإجراءات القيام بها في (الفرع الأول) ثم نتطرق أيضا إلى مفهوم تسجيل الأصوات وإجراءات القيام بها في (الفرع الثاني).

الفرع الأول: مفهوم اعتراض المراسلات واجراءات القيام بها: سنقوم أولا بتوضيح ما المقصود باعتراض المراسلات، وثانيا كيفية القيام بهذا الإجراء التقني.

أولا: مفهوم اعتراض المراسلات: يقصد باعتراض المراسلات على أنه:" إجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطات القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة، ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث وتتم بواسطة الوسائل السّلكية واللاّسلكية"[1]. إذا تقوم جهات البحث والتحري بالتتبع السرّي والمتواصل للمشتبه فيه قبل وبعد ارتكابه للجريمة ثم القبض عليه متلبسا. من جانب آخر أغفل المشرع الجزائري تعريف اعتراض المراسلات ولكنه بالمقابل اكتفى بتنظيم هذه العملية بموجب المادة (65 مكرر5) من (ق.إ.ج.ج) على:" إذا اقتضت ضروريات التحري في الجريمة المتلبّس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية

[1] سارة قادري، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماستر أكاديمي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر ،2014، ص32.

للمعطيات أو جرائم تبييض الأموال أو الارهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد ، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاّسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص...".

بالرجوع لنص المادة (46) من التعديل الدستوري المؤرخ في:2016/03/06 التي تنص على :" لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميهما القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة. لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم... ". وعليه يضمن الدستور الجزائري سرّية المكالمات الهاتفية وكل الاتصالات بأشكالها المختلفة(مكالمات باستعمال الهاتف الخلوي أو مكالمات مرئية باستعمال شبكة الإنترنت أو خطابات أو برقيات أو مستندات...إلخ) من التنصت والمراقبة أو النشر أو الاطلاع أو الاعتراض تحت طائلة العقوبات. كما نص المشرع أيضا على سرّية المراسلات بموجب نص المادة (105) الفقرة الأخيرة من القانون رقم:2000-03المؤرخ في:2000/08/05 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاّسلكية، كما نص أيضا على سرّية البيانات المتعلقة بالتصديق الإلكتروني بنص المادتين(42 -43) من القانون رقم:15-04 المؤرخ في:2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، حيث تنص المادة (42) على:" يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سريّة البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة..."[1]، حيث يهدف المشرع الجزائري إلى إضفاء حماية خاصة على الاتصالات بين الأشخاص مهما كان نوعها تماشيا مع المبادئ الدستورية والمواثيق الدولية المتعلقة بحرمة الحياة الخاصة للأفراد.

من جهة أخرى عرفت المادة (9/08) من القانون رقم:2000- 03 المؤرخ في:2000/08/05 يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاّسلكية: "يقصد في مفهوم هذا القانون...شبكة المواصلات السلكية واللاّسلكية: كل منشأة أو مجموعة منشآت تضمن إما التراسل و إما تراسل و إرسال إشارات المواصلات السلكية واللاّسلكية و كذا تبادل معلومات التحكم والتسيير المشتركة ما بين النقط الطرفية لهذه الشبكة"، كما نصت المادة (10/08) على أنواع

[1] المادتان (43-42) من القانون رقم:15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

الشبكات فقد تكون شبكة داخلية أو شبكة خاصة[1]. من جانب آخر أورد المشرع الجزائري تعريفا للاتصالات الإلكترونية بموجب نص المادة (02/و) من القانون رقم:09-04 السابق ذكره على أنها:" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية."

وباستقراء نصوص المواد (100-107) من (ق.إ.ج.ف)[2]، يتبين أن اعتراض المراسلات تتعلق بتلقي مراسلة مهما كان نوعها بغض النظر عن وسيلة إرسالها وتلقيها سلكية أو غير سلكية يتم تثبيتها وتسجيلها على دعامة الكترونية *(Support)* أو ورقية[3].كما عرفت لجنة الخبراء للبرلمان الأوروبي المنعقدة بستراسبورغ بتاريخ:2006/10/06 حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية اعتراض المراسلات على أنها: "عملية مراقبة سرية المراسلات السلكية واللاّسلكية، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الاشخاص المشتبه فيهم أو في مشاركتهم في ارتكاب الجريمة"[4].

ورغم هذه الأهمية لم يحدد المشرع الجزائري مفهوم اعتراض المراسلات، إلا أنه تناول في المادة(65 مكرر5 -65 مكرر10) من (ق.إ.ج.ج) سلطة تقدير اللّجوء إلى اعتراض المراسلات وأطر التحقيق الممارس فيها وأنواع الجرائم التي تستعمل فيها وشروط الإذن باعتراض المراسلات الشكلية ومضمونه ومدته. فمن خلال استقراء نص المادة (65 مكرر5) يقصد بعملية اعتراض المراسلات، اعتراض أو تسجيل أو نسخ المراسلات التي تتم باستعمال وسائل الاتصال السلكية واللاسلكية قصد رصد الدليل الذي يتم من خلاله إدانة المجرم الإلكتروني خاصة أنه يتم وضع الترتيبات التقنية دون علم وموافقة المشتبه فيه، غير أن المشرع الجزائري خصّ بالذكر المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاّسلكية دون الرسائل والخطابات والطرود

---

1 المادة (08/12-9) من القانون رقم:2000- 03 يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية.

2 ***Article 100 du (CPPF) :***

"En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications. Ces opérations sont effectuées sous son autorité et son contrôle. La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours".

3 عبد المجيد جباري، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة والنشر والتوزيع الجزائر،2012، ص62 .

4 رشيدة بوكر، المرجع السابق، ص442.

لدى مكاتب البريد، كما أنه لم يُول اهتماما لأداة الاعتراض فقد تكون تقليدية أو بأحدث الوسائل التكنولوجية المتوفرة[1] .

من جهة أخرى، هل يقصد المشرع الجزائري الاتصالات الهاتفية[2] فقط أم تلك المراسلات التي تتم بالحاسوب أين يتبادل فيها المتهم المراسلات مع الغير؟. في واقع الأمر ساهمت تقنية الاتصالات الحديثة بكافة أشكالها في ارتكاب الجرائم المستحدثة، حيث أجازت المادة (03) من(إ.أ.م.إ.م) الاعتراض الشرعي لكافة أشكال النقل الإلكتروني للبيانات سواء عن طريق التليفون أو الفاكس أو البريد الإلكتروني، حيث تشمل الاتصالات محل الاعتراض المحتوى غير المشروع أو الدليل على الأفعال الإجرامية الخطيرة المنصوص عليها في القانون الداخلي لكل دولة. مما يستوجب ضرورة اعتراض المراسلات الإلكترونية المتبادلة عبر الحاسوب لدرء خطر الجريمة وملاحقة الجناة، وهذا ربما ما قصده المشرع صراحة من خلال أحكام اعتراض المراسلات السلكية واللاّسلكية، وأيضا بموجب احكام القانون رقم:09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3]، حيث أجاز المشرع وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها[4] والقيام أيضا بإجراءات التفتيش والحجز داخل منظومة معلوماتية[5].

لكن كيف تتم عملية اعتراض المراسلات على المستوى الإجرائي؟ هذا ما سنتاوله فيما يأتي:

ثانيا: إجراءات اعتراض المراسلات: نتناولها وفق التقسيم الآتي:

1- تحديد مجال اعتراض المراسلات: نصت المادة(65 مكرر 5) من (ق.إ.ج.ج) على الجرائم التي يجوز القيام فيها بهذه العملية وهي:

- جرائم المخدرات.

---

[1] فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرّب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة قسنطينة1، العدد:33، جوان 2010، ص237.

[2] يُثار التساؤل بالنسبة لمسألة التصنت التليفوني، لكونها تشكل انتهاكا لحرمة المراسلات التي كفلها الدستور، وما إذا كان يمكن لقاضي التحقيق أن يأمر بالتصنت على المحادثات التليفونية. حيث لم يرد في قانون الإجراءات الجزائية الجزائري أي نص في هذه المسألة ، كما لم تثر هذه المسألة أيضا أمام المحكمة العليا، وعليه يعتبر هذا الإجراء شرعيا متى أمر به قاضي التحقيق استنادا الى نص المادة (1/68) من (ق.إ.ج.ج) التي تسمح لقاضي التحقيق أن يقوم بجميع الإجراءات التي يراها مناسبة للكشف عن الحقيقة بالتحري عن أدلة الاتهام وأدلة النفي، أحسن بوسقيعة، التحقيق القضائي، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط5، 2004، ص93.

[3] جميلة محلق، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، جامعة باجي مختار، عنابة، الجزائر، العدد42، جوان2015، ص178 .

[4] المادة (03) من القانون رقم:09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[5] المرجع نفسه، المواد من:(09-05).

- الجريمة المنظمة العابرة للحدود الوطنية.

- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

- جرائم تبييض الأموال.

- جرائم الإرهاب.

- الجرائم المتعلقة بالتشريع الخاص بالصرف: وهو الأمر رقم: 96-22 المؤرخ في 1996/07/09 المتمم والمعدل بالأمر رقم: 03-01 المؤرخ في:2003/02/19 .

- جرائم الفساد المحددة بالقانون رقم:06-01 المؤرخ في: 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته.

2- الجهة القضائية التي يجوز لها بمنح الإذن للقيام بهذه العملية : حسب ما ورد في نص المادة (65 مكرر 5) فإن منح الإذن للقيام بهذه العمليات مقتصر على كل من:

- **وكيل الجمهورية :** يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة له.

- **قاضي التحقيق :** في حالة فتح تحقيق قضائي فإن العمليات المذكورة في المادة (65 مكرر 05) تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة(65 مكرر6/5).

3-الأماكن التي يسمح فيها بالاعتراض: لم يحدد المشرع الجزائري بدقة الأماكن التي ستتم فيها عملية الاعتراض، بل جاء النص على عمومه، حيث نصت المادة (65 مكرر 05) على :"...في أماكن خاصة أو عمومية..." دون استثناء فقد يكون منزلا أو مقهى للإنترنت أو شركة...إلخ مخالفا في ذلك المشرع الفرنسي الذي أورد استثناءات في هذا الشأن بموجب المادة(706 -96) من (ق.إ.ج.ف) مثل: المحلات التي تحتوي على مؤسسات إعلامية والمحلات ذات الطابع المهني للأطباء وسيارات النواب والمحامين...إلخ[1]. حيث سمح المشرع الجزائري بالدخول إلى تلك الأماكن

---

[1] ***Article 706-96 du (CPPF) :***

"Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles== ==prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules

ووضع الوسائل اللازمة لاعتراض المراسلات حتى بغير علم وموافقة أصحابها وحتى خارج الآجال المنصوص عليها في المادة (47) من(ق.إ.ج.ج)[1] بمعنى أنها تكون في أي وقت.

4- مضمون الإذن ومدتـه : يتضمن الإذن المذكور في المادة (65 مكرر 5) الممنوح سواء من طرف وكيل الجمهورية أو قاضي التحقيق على كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سواء كانت سكنية أو غيرها، وكذا الجريمة التي تبرر اللّجوء إلى هذه التدابير ومدتها، حيث تنص المادة (65 مكرر7) على:" يجب أن يتضمن الإذن المذكور في المادة 65 مكرر5 أعلاه كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن السكنية المقصودة أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها. يسلم الإذن مكتوبا لمدة أقصاها أربعة(4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية".

من خلال هذه المادة يمكن أن نستتشف الشروط الشكلية والزمنية للإذن وهي :

- أن يكون الإذن مكتوبا.

- ذكر جميع العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة، وذلك بالتحديد الدقيق للاتصال المراد مراقبته أو المراسلة التي سيتم اعتراضها وكذا المكان الذي يتم فيه وضع الترتيبات التقنية.

- ذكر الجريمة التي تبرّر اللّجوء إلى هذه العملية وهي إحدى الجرائم المذكورة على سبيل الحصر في نص المادة(65 مكرر 5) من (ق.إ.ج.ج) .

- ذكر المدة التي تتم خلالها العملية على ألا تتجاوز مدة أربعة (4)أشهر قابلة للتجديد بالشروط نفسها.

4- كيـف تتـم العمليـة: يتم اعتراض المراسلات بتسخير أعوان مصالح الاتصالات السلكية واللاّسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65

---

privés ou publics, ou de l'image d'une ou plusieurs personnes se trouvant dans un lieu privé. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction…

La mise en place du dispositif technique mentionné au premier alinéa ne peut concerner les lieux visés aux articles 56-1,56-2 et 56-3 ni être mise en œuvre dans le véhicule, le bureau ou le domicile des personnes visées à l'article 100-7…".

[1] المادة (47) (ق.إ.ج.ج).

مكرر8)[1]. كما يلزم ضابط الشرطة القضائية المأذون له أو المُناب من طرف القاضي المختص بتحرير محضر عن كل عملية اعتراض وتسجيل المراسلات، وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط، ويحدد بالضبط تاريخ وساعة بداية هذه العمليات والانتهاء منها، كما يمكن ترجمة المراسلات التي تتم باللّغات الأجنبية، ويسجل كل هذا في محضر يودع بالملف وهذا وفقا لنص المادتان(65 مكرر9- 65 مكرر10) من (ق.إ.ج.ج). كما تجدر الإشارة إلى أن هذه العملية تتم دون المساس بالسر المهني المنصوص عليه في المادة (45) من القانون نفسه. وذلك باتخاذ جميع التدابير اللاّزمة لضمان احترام السر وفق نص المادة(65 مكرر6) من (ق.إ.ج.ج).

في هذا المجال يعتبر البريد الإلكتروني *(e-mail)* من أهم وسائل الاتصال الحديثة التي توفرها شبكة الإنترنت، لما يمتاز به من أمان وسرعة في نقل المستندات والرسائل والملفات وتخزينها، كما أنه يتمتع بالحماية القانونية نظرا لأهميته البالغة، حيث صار مستخدما بكثرة مما يجعله عرضة للاختراق من قبل قراصنة الحاسوب، كما أنه يستعمل أيضا من قبل المجرمين للتواصل فيما بينهم وإعداد خططهم بعيدا عن أعين الأجهزة الأمنية، وكما أسلفنا أجاز المشرع اعتراض المراسلات ومن بينها التي تتم عن طريق البريد الإلكتروني حينما يتطلب الأمر كشف الجرائم الإلكترونية ومرتكبيها[2].

وأخيرا أظهرت التشريعات الحديثة فائدة كبيرة في هذا الاجراء رغم أنه يتضمن اعتداء جسيما على حرمة الحياة الخاصة، ولكنه يباح استثناء بغرض الوصول إلى الحقيقة بخصوص الجرائم الإلكترونية[3]. فبإمكان ضباط الشرطة القضائية اعتراض هذه الاتصالات عن بعد، سواء كانت سلكية أو لاسلكية وذلك باستعمال أجهزة تكنولوجية حديثة، بما يمكنهم من استخلاص الدليل الرقمي[4].

الفرع الثاني: تسجيل الأصوات واجراءات القيام به:

يعتبر إجراء تسجيل الأصوات من الإجراءات الخفية مثل اعتراض المراسلات، الهدف منه تمكين أجهزة البحث والتحري من اكتشاف الحقيقة، سنتناول أولا مفهوم تسجيل الأصوات ثم نتطرق ثانيا إلى الإجراءات المتعلقة به.

أولا: مفهوم تسجيل الأصوات: يُعرف تسجيل الأصوات بأنه:" النقل المباشر والآلي للموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية بما تحمل من عيوب في النطق إلى شريط التسجيل لحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي بحيث يمكن إعادة سماع

---

[1] حيث تنص المادة (65مكرر8) من (ق.إ.ج.ج) على:" يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أُذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي يُنيبه، أن يُسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاّسلكية للتكفل بالعمليات التقنية للعمليات المذكورة في المادة 65 مكرر 5 أعلاه".

[2] زيدان زيبحة، المرجع السابق، ص159.

[3] رشيدة بوكر، المرجع السابق، ص445.

[4] نصر شومان، المرجع السابق، ص154.

الصوت والتعرف على مضمونه"[1]. أو هي تلك:" المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان خاص أو عام، ويتم ذلك عن طريق حفظ الحديث على جهاز معد لذلك للاستماع إليه مرة أخرى[2]. وعليه واستنتاجا من التعريفين السابقين يعتبر التسجيل الصوتي نقل الموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية إلى شريط تسجيل بحيث يمكن إعادة سماع الصوت للتعرف على مضمونه وإدراك خواصه التي تشكل عناصر المقارنة عند مضاهاتها على صوت الشخص المنسوب إليه، مما يتيح تقرير إسناده أو نفي ذلك، وهو من الوسائل الملائمة لضبط الحقيقة[3]. كما تتم هذه العملية باستخدام وسائل تقنية خاصة[4] لها صلة مباشرة بنوعيها السلكية واللاّسلكية، والتي من خلالها يتم بث الكلام المتفوه به وتثبيته واستغلاله في التحريات، وهو إجراء تحقيقي تأمر به السلطة القضائية خلسة وينتهك سرية الأحاديث الخاصة بغية الحصول على دليل غير مادي للجريمة[5].

فتسجيل الأصوات يقصد به أيضا تسجيل أحاديث المتهم وشركائه خلسة عن واقعة معينة من الوقائع المنصوص علي بموجب المادة (65 مكرر 5) من (ق.إ.ج.ج)، فبعد أن أعطى المشرع للمتهم الحق في السكوت، فإنه أورد استثناء على هذا الحق أين أصبح من الممكن أخذ اعتراف المتهم ضد نفسه بشكل خفي ودون رضاه وموافقته عن طريق تسجيل كل ما يفوه به من أحاديث سرية[6].

بالرجوع إلى نص المادة(65 مكرر5) من(ق.إ.ج.ج) التي تنص على:" اذا اقتضت ضروريات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض

---

[1] سارة قادري، المذكرة السابقة، ص34.

[2] جميلة محلق، المقال السابق، ص178.

[3] عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص779.

[4] من الوسائل الحديثة في هذا المجال آلات ابتكرها العلماء يمكنها التقاط الأصوات عن بعد بمجرد توجيهها نحو مصدر الصوت، كما يمكنها فصل الأصوات المسموعة عن بعضها البعض لكي تتيح لمستعملها انتقاء الصوت الذي يريد سماعه من بين الأصوات المتوفرة في المكان، وهذا ما يساعد أجهزة البحث والتحري في القيام بمراقبة فعّالة ووقائية للحد من انتشار الجريمة وخاصة المستحدث منها، راجع نصر شومان، المرجع السابق، ص 155.

[5] حافظ بن زلاط، التنصت الهاتفي في ظل قانون الإجراءات الجزائية، بحث متوفر على الموقع الرسمي لمجلة (القانون والأعمال) لسنة 2015 على الرابط الآتي:

http://www.droitetentreprise.org/web/%D8%A7%D9%84%D8%AA%D9%86%D8%B5%D8%AA-%D8%A7%D9%84%D9%87%D8%A7%D8%AA%D9%81%D9%8A-%D9%81%D9%8A-%D8%B8%D9%84-%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%A5%D8%AC%D8%B1%D8%A7%D8%A1%D8%A7%D8%AA-%D8%A7/ ، تاريخ الاطلاع:2016/04/08 على الساعة: 18:25.

[6] فوزي عمارة، المقال السابق، ص237.

الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد ، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاّسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية، من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية..."

إن الهدف من هذا الإجراء هو إظهار الحقيقة لكشف الجريمة ومرتكبها[1]، حيث أجاز المشرع وضع الترتيبات التقنية دون علم وموافقة المعنيين من أجل تسجيل الحديث المتفوه به في الأماكن العامة أو الخاصة. وبذلك أخذ المشرع الجزائري بالمذهب الموضوعي حيث تُعد طبيعة الحديث أساس الحماية الجنائية بغض النظر عن المكان الذي يجرى فيه وهو المعيار الذي أخذ به المشرع الفرنسي أيضا[2]، فيقوم ضابط الشرطة القضائية بمتابعة المكالمات الهاتفية والأحاديث الخاصة والسرية سواء في أماكن خاصة أو عامة، ويتطلب ذلك وضع رقابة على الهواتف ونقل الأحاديث وتسجيلها ويتم ذلك عن طريق وضع ميكروفونات حسّاسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة وقد يتم أيضا عن طريق التقاط إشارات لاسلكية إذاعية[3]. كما يأخذ حكم الحديث الخاص والسرّي ذلك الحديث الذي يجري في مكان خاص أو مكان عام وكان شخصيا ويتضمن أدق الأسرار أين يعبّر الإنسان عن نفسه وينقل ذلك إلى شخص آخر، مما قد يشكل دليلا لإظهار الحقيقة[4].

ثانيا: اجراءات تسجيل الأصوات: ويتم ذلك كما يأتي:

---

[1] أسهم تسجيل الرئيس الأمريكي الأسبق (ريتشارد نيكسون) لما يدور من أحاديث داخل البيت الأبيض الأمريكي ضمن ما يعرف بفضيحة "ووتر جيت" *(Watergate scandal)*، بإلقاء شكوك حول محاولته تغيير شرائط التسجيل المتعلقة بهذه القضية مما تسبب في إنهاء حياته السياسية، راجع، عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص781.

[2] جميلة محلق، المقال السابق، ص179.

[3] إن تسجيل الصوت وإعادة إنتاجه هو الكتابة الكهربية أو الميكانيكية للموجات الصوتية وإعادة تكونيها، ويتم بطريقتين: التسجيل التناظري والتسجيل الرقمي. ويتم التسجيل التناظري بواسطة طبقة مصدح صغيرة يمكنها اكتشاف التغيرات في الضغط الجوي، حيث تستشعر إبرة التسجيل الانخفاضات في التسجيل، حيث تسبب الموجات الصوتية اهتزاز طبقة المصدح "الميكروفون" ويتم تحويلها إلى تيار كهربائي متغير، والذي يتحول بعد ذلك إلى مجال مغناطيسي متغير بواسطة مغناطيس كهربي، مما يؤدي إلى إنشاء تمثيل للصوت. أما التسجيل الرقمي فيخزن الصوت كمجموعة من أرقام ثنائية وهي ذات جودة أعلى بسبب التنسيق الرقمي، لمزيد من التفاصيل، يرجى زيارة الموقع الآتي:

https://ar.wikipedia.org/wiki/%D8%AA%D8%B3%D8%AC%D9%8A%D9%84_%D8%A7%D9%84%D8%B5%D9%88%D8%AA_%D9%88%D8%A5%D8%B9%D8%A7%D8%AF%D8%A9_%D8%A5%D9%86%D8%AA%D8%A7%D8%AC%D9%87 ، تاريخ الاطلاع:2016/04/09 على الساعة:06:00.

[4] فوزي عمارة، المقال السابق، ص237.

1- تحديد مجال تسجيل الأصوات: نصت المادة(65 مكرر5) سالفة الذكر على الجرائم التي يجوز القيام فيها بهذه العملية وهي: جرائم المخدرات- الجريمة المنظمة العابرة للحدود الوطنية - الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...إلخ.

2- منح الإذن للقيام بهذه العملية: حسب ما ورد في نص المادة(65 مكرر 5) فإن منح الإذن للقيام بهذه العمليات مقتصر على كل من:

- **وكيل الجمهورية** : يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفذ العمليات المأذون بها تحت مراقبته المباشرة.

- **قاضي التحقيق** : في حالة فتح تحقيق قضائي فإن العمليات المذكورة في المادة(65 مكرر5) تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة(65 مكرر6/5) من (ق.إ.ج.ج).

3-أماكن تسجيل الأصوات: لم يحدد المشرع الجزائري بدقة الأماكن التي ستتم فيها عملية تسجيل الأصوات، بل جاء النص على عمومه، حيث نصت المادة (65 مكرر 5)على :"...في أماكن خاصة أو عمومية..."، حيث سمح المشرع الجزائري بالدخول إلى تلك الأماكن ووضع الوسائل اللازمة لتسجيل الأصوات كتركيب الميكروفونات حتى بغير علم وموافقة أصحابها وحتى خارج الآجال المنصوص عليها في المادة (47) من (ق.إ.ج.ج).

4- مضمون الإذن ومدتـه : يتضمن الإذن المذكور في المادة(65 مكرر 5) الممنوح سواء من طرف وكيل الجمهورية أو قاضي التحقيق على كل العناصر التي تسمح بالتعرف على الأشخاص المراد التقاط أو بث أو تسجيل أحاديثهم، وكذا الأماكن المقصودة سواء كانت عامة أو خاصة وكذا الجريمة التي تبرّر اللّجوء إلى هذه التدابير ومدتها، حيث تنص المادة (65 مكرر7) على:" يجب أن يتضمن الإذن المذكور في المادة 65 مكرر5 أعلاه كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرّر اللّجوء إلى هذه التدابير ومدتها. يسلم الإذن مكتوبا لمدة أقصاها أربعة(4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية".

5- كيـف تتـم العمليـة: تتم عملية تسجيل الأصوات بتسخير أعوان مصالح الاتصالات السلكية واللاّسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة(65 مكرر8) سالفة الذكر. كما يلزم ضابط الشرطة القضائية المأذون له أو المُناب من

طرف القاضي المختص بتحرير محضر عن كل عملية تسجيل الأصوات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط، ويحدد بالضبط تاريخ وساعة بداية هذه العمليات والانتهاء منها.

إن التسجيلات الصوتية الحديثة لها حجية كبيرة في الإثبات الجنائي، لأن التقنيات الإلكترونية المتطورة للتسجيل لا تحتمل الخطأ، وبإمكان الخبراء كشف أي تعديل أو تلاعب بواسطة تقنية عالية الكفاءة، كما يجب على القاضي قبل ترسيخ قناعته التأكد من أن الصوت المسجل يخص المتهم عن طريق ما يعرف ببصمة الصوت، وأن لا يكون قد حدث تعديل أو مونتاج على التسجيل، كما يجب أن يكون التسجيل واضحا[1].

المطلب الثاني: التقاط الصوّر

إن عملية التقاط الصور باعتبارها إحدى وسائل البحث والتحري الحديثة، هي استثناء عن المبدأ العام الذي يمنع التقاط الصور دون رضا صاحبها لما فيها من مساس بحرمة الحياة الخاصة المحمية قانونا، سنتناول مفهوم التقاط الصور في (الفرع الأول)، ثم نتناول إجراءاته في (الفرع الثاني).

الفرع الأول: مفهوم التقاط الصور:

تعتبر عملية التقاط الصور الفوتوغرافية من الإجراءات الجديدة التي جاء بها المشرع الجزائري لمكافحة الجرائم المستحدثة ومنها الجرائم الإلكترونية، غير أنه ومثل الإجراءات السابقة لم يتطرق إلى تعريف هذا الإجراء، وإنما نص على مجال تطبيقه وتوضيح إجراءات القيام بذلك. يقوم هذا الإجراء أساسا على استخدام الكاميرات، أو أجهزة خاصة لالتقاط صورة للمشتبه فيه على الحالة التي كان عليها وقت التصوير بغرض استخدام هذه الصورة كدليل مادي، على اعتبار أن عدسة الكاميرا أصبحت من الأساليب العالمية والمطلوبة لإثبات الحالة بما تنقله من صور حيّة لحادثة معينة[2].

لقد شاع اليوم استخدام كاميرات رقمية بغرض المراقبة في الأماكن العامة والخاصة كالبنوك والمطارات وماكينات الصرف الآلي والمحلات والمستشفيات وقاعات الانتظار...إلخ قصد ضبط الجرائم وإثباتها[3]، ويكون الاطلاع على صور هذه الكاميرات في حالات وقوع الجرائم بأمر من المحكمة ولاشك أن ذلك يثير قضايا تتعلق بالخصوصية الشخصية. لذا يرى جانب من الفقه أن تركيب هذه الكاميرات يكون في الأماكن العامة فقط وبترخيص قانوني[4].

---

[1] عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص781.

[2] فوزي عمارة، المقال السابق، ص238.

[3] سارة قادري، المذكرة السابقة، ص39.

[4] عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص782.

بالرجوع لنص المادة (65 مكرر5) من (ق.إ.ج.ج) التي تنص على:" اذا اقتضت ضروريات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

– وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوّه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص...".

وعليه يربط هذا الإجراء الشخص أو الأشخاص في مكان واحد وفي وقت واحد، خاصة في ظل التطور التكنولوجي الرّقمي الذي يسمح بالتصوير ليلا وبجودة عالية من خلال الكاميرا ذات العدسات فائقة التكبير والتي تستخدم أيضا الأشعة تحت الحمراء بما يمكّن ضابط الشرطة القضائية من التقاط الصور الثابتة أو المتحركة للمشتبه فيه خلال جميع مراحل البحث والتحري[1].

الفرع الثاني: إجراءات التقاط الصور:

نتطرق إليها كما يأتي:

أولا: تحديد مجال التقاط الصور : نصت المادة (65 مكرر 5) سالفة الذكر على الجرائم التي يجوز القيام فيها بهذه العملية وهي:

– جرائم المخدرات .

– الجريمة المنظمة العابرة للحدود الوطنية .

–الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

– جرائم تبييض الأموال.

– جرائم الإرهاب.

– الجرائم المتعلقة بالتشريع الخاص بالصرف.

– جرائم الفساد.

ثانيا: منح الإذن للقيام بهذه العملية : حسب ما ورد في نص المادة(65 مكرر 5) فإن منح الإذن للقيام بهذه العمليات مقتصر على كل من:

---

[1] نصر شومان، المرجع السابق، ص154.

– **وكيل الجمهورية:** يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفذ العمليات المأذون بها على هذا الأساس وتحت المراقبة المباشرة له.

– **قاضي التحقيق:** في حالة فتح تحقيق قضائي فإن العمليات المذكورة في المادة(65 مكرر 5) تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة (65 مكرر 5 /6)

– **أماكن التقاط الصور:** على خلاف تسجيل الأصوات التي تتم في أماكن عمومية أو خاصة استثنى المشرع الجزائري التقاط الصور في الأماكن العمومية، غير أنه سمح بهذا التدبير في بعض القوانين الخاصة كالترصّد الإلكتروني والاختراق بموجب المادة (56) من القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته[1] .

ثالثا: مضمون الإذن ومدتـه: يتضمن الإذن المذكور في المادة(65 مكرر 5)الممنوح سواء من طرف وكيل الجمهورية أو قاضي التحقيق على كل العناصر التي تسمح بالتعرف على الأشخاص المراد التقاط الصور لهم والأماكن المقصودة سواء كانت عامة أو خاصة، وكذا الجريمة التي تبرّر اللّجوء إلى هذه التدابير ومدتها، حيث تنص المادة (65 مكرر7) على:" ... يسلم الإذن مكتوبا لمدة أقصاها أربعة(4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية".

رابعا: كيـف تتـم العمليـة: تتم عملية التقاط الصور بتسخير أعوان مصالح الاتصالات السلكية واللاّسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65 مكرر8) سالفة الذكر. كما يلزم ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بتحرير محضر عن كل عملية التقاط الصور، وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط، ويحدد بالضبط تاريخ وساعة بداية هذه العمليات والانتهاء منها، وهذا بموجب المادتين(9 –10) من (ق.إ.ج.ج).

بعد دراستنا لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وما تمثله هذه الإجراءات الجديدة في مكافحة الجرائم المستحدثة ومنها الجرائم الإلكترونية، إلا أنه يمكن ملاحظة بعض الإشكالات القانونية والعملية في تطبيقها[2] نلخصها كما يأتي:

---

[1] تنص المادة (56) من القانون رقم:06-01 المؤرخ في: 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته على:" من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون، يمكن اللجوء إلى التسليم المراقب أو اتباع أساليب تحر خاصة كالترصد الإلكتروني والاختراق، على النحو المناسب وبإذن من السلطة القضائية المختصة"، (ج. ر) رقم:14 المؤرخة في:2006/03/08 ص12.

[2] عبد المجيد جباري، المرجع السابق، ص ص67-68.

أ- **الإشكالات القانونية:** تتمثل في:

- لم تبين النصوص القانونية الوسائل القانونية التي يمكن من خلالها استعمال الوسائل التقنية التكنولوجية للقيام بهذه العمليات.

- عدم تحديد نوع المؤسسات المسخرة وكذا المصاريف والأتعاب.

ب- الاشكالات العملية: تتمثل في:

- مدى توافر الوسائل التقنية لاعتراض المراسلات وتثبيتها، وهي عادة ما تكون وسائل تقنية ذات كفاءة عالية.

- مدى توافر التعداد البشري الكافي والمؤهل.

- إمكانية التلاعب وإتلاف المراسلات والأصوات المثبتة على دعامات إلكترونية أو مغناطيسية، لذا لابد من إيجاد احتياطات خاصة لتخزينها.

المطلب الثالث: التسرّب

يعتبر إجراء التسرّب من الإجراءات الجديدة الهامة التي جاء بها المشرع الجزائري لمكافحة أنواع معينة من الجرائم المستحدثة ذات الطبيعة الخاصة ومنها الجرائم الإلكترونية، حيث نظم أحكام التسرّب في الفصل الخامس من (ق.إ.ج.ج) بموجب المواد من(65 مكرر 11 - 65 مكرر 18) وتمت الإشارة أيضا إلى المادة (65 مكر 5) فيما يخص الجرائم المرتبطة بهذا الإجراء، سنتطرق إلى مفهوم التسرّب في (الفرع الأول)، ثم نتناول الشروط الشكلية والموضوعية وآثاره في (الفرع الثاني).

الفرع الأول: مفهوم التسرّب:

استحدث المشرع الجزائري إجراء التسرّب بموجب المادة (65 مكرر11) من (ق.إ.ج.ج) التي تنص على:" عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر5) أعلاه ، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرّب ضمن الشروط المبينة في المواد أدناه".

وبخلاف إجراءات التحري سابقة الذكر التي لم يعرفها المشرع الجزائري، أورد تعريف التسرّب بموجب المادة (65 مكرر12) من (ق.إ.ج.ج) التي تنص على:" يقصد بالتسرّب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف. يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة (65 مكرر14) أدناه، ولا يجوز تحت طائلة البطلان، أن تشكل هذه الأفعال

تحريضا على ارتكاب الجرائم". كما حدد المشرع نطاق تطبيق التسرّب بموجب المادة (65 مكرر5) سالفة الذكر والتي من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

يلاحظ من خلال التعريف السابق أن التسرّب عملية تتسم بالتعقيد، فهو من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية، وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرّب بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقة وتقديم المتسرّب لنفسه على أنه فاعل أو شريك[1]، ويمكن تصور عملية التسرّب في نطاق مكافحة الجريمة الإلكترونية دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي واشتراكه مثلا في غرف الدردشة أو حلقات النقاش والاتصال المباشر في كيفية القيام بنشر الفيروسات أو اختراق الأنظمة المعلوماتية مستخدما في ذلك هوية مستعارة بقصد الإيقاع بالمجرم الإلكتروني.

من جانب آخر تطرقت عديد التشريعات إلى النص على إجراء التسرب لأهميته، إذ يعتبر وسيلة فعّالة في مجال البحث والتحري عن الجرائم، ومنها التشريع الفرنسي الذي نص عليه بموجب المواد من(706-81)إلى(706-87) من (ق.إ.ج.ف)[2]. إن هذا الإجراء يبدو في البداية غير مستساغ وخطير على حقوق وحريات الأشخاص، حيث يستعمل المتسرّب أساليب غير مشروعة من انتحال لهوية مستعارة وعند الاقتضاء ارتكاب جرائم تبديدا للشكوك ونَيلا لثقة الجماعة الإجرامية[3] إلا أن المشرع أحاطه بجملة من الضوابط تجعله يتم وفق الشروط الشكلية والقانونية المطلوبة، والتي سنتناولها في الفرع الموالي.

الفرع الثاني: الشروط الشكلية والموضوعية للتسرّب وآثاره:

كما قلنا سلفا يعتبر التسرّب من أخطر الإجراءات على حرمة الحياة الخاصة للأفراد، مما استوجب على المشرع ضبطه بجملة من الشروط الشكلية والموضوعية نتناولها كما يأتي:

أولا: الشروط الشكلية: يجب أن تتوفر في التسرّب الشروط الشكلية الآتية:

---

[1] سارة قادري، المذكرة السابقة، ص42.

[2] ***Article 706-81 du (CPPF) :***

"Lorsque les nécessités de l'enquête ou de l'instruction concernant l'un des crimes ou délits entrant dans le champ d'application des articles 706-73 et 706-73-1 le justifient, le procureur de la République ou, après avis de ce magistrat, le juge d'instruction saisi peuvent autoriser qu'il soit procédé, sous leur contrôle respectif, à une opération d'infiltration dans les conditions prévues par la présente section".

[3] فوزري عمارة، المقال السابق، ص246.

1- الإذن القضائي: تنص المادة (65 مكرر11) من (ق.إ.ج.ج) على:" عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر5) أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرّب ضمن الشروط المبينة في المواد أدناه". وعليه فالجهة القضائية المختصة بإصدار الإذن هو وكيل الجمهورية أو قاضي التحقيق، ومنه لا يجوز لضابط أو أعوان الشرطة القضائية القيام به حماية للحقوق المكرسة دستوريا.

2- **يجب أن يكون الإذن مكتوبا:** وهذا وفق نص المادة (65 مكرر15) التي تنص على: "يجب أن يكون الإذن المسلم تطبيقا للمادة (65 مكرر11) أعلاه، مكتوبا... وذلك تحت طائلة البطلان" ذلك أن الأصل في العمل الإجرائي هو الكتابة. وفقا لنص المادتين (138-139) من (ق.إ.ج)[1].

3- **ذكر اسم الضابط المشرف:** وهو ما نصت عليه المادة(65 مكرر15) بقولها:" يجب أن يكون الإذن المسلّم تطبيقا للمادة 65 مكرر 11 أعلاه، مكتوبا... وذلك تحت طائلة البطلان. تذكر في الإذن الجريمة التي تبرّر اللّجوء لهذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته...".

4- **مدة التسرّب:** حددتها المادة(65 مكرر3/15) حيث تنص على:"...ويحدد هذا الإذن مدة عملية التسرّب التي لا يمكن أن تتجاوز أربعة(4) أشهر..."، غير أنه ومراعاة لمقتضيات التحقيق الابتدائي يمكن تجديد هذه المدة ضمن نفس الشروط الشكلية والزمنية السابقة. وحفاظا على حياة العون المتسرّب من الخطر إضافة إلى الأشخاص المُسخّرين، أجاز المشرع للقاضي الذي رخص بعملية التسرّب أن يأمر في أي وقت بوقفها قبل انقضاء مدتها، وذلك إذا وصل إلى علمه أن معلومات تفيد باحتمال كشف العملية من طرف المجموعة الإجرامية[2]. إلاّ أنه إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في رخصة التسرّب وفي حالة عدم تمديدها يمكن للعون المتسرّب مواصلة نشاطاته للوقت الضروري لتوقيف عملية التسرّب في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا على أن لا يتجاوز ذلك مدة أربعة(4) أشهر مع وجوب إخطار القاضي المصدر

---

[1] حيث تنص المادة (138) من (ق.إ.ج.ج) على: "يجوز لقاضي التحقيق أن يكلف بطريق الإنابة القضائية أي قاض من قضاة محكمته أو أي ضابط من ضباط الشرطة القضائية المختصة بالعمل في تلك الدائرة أو أي قاض من قضاة التحقيق بالقيام بما يراه لازما من إجراءات التحقيق في الأماكن الخاضعة للجهة القضائية التي يتبعها كل منهم. ويذكر في الإنابة القضائية نوع الجريمة موضوع المتابعة وتؤرخ وتوقع من القاضي الذي أصدرها وتمهر بختمه...".

[2] عبد المجيد جباري، المرجع السابق، ص60.

للرخصة في أقرب الآجال، إذ أجاز المشرع للقاضي تجديدها لمدة أربعة (4) أشهر على الأكثر وهذا حسب نص المادة(65 مكرر 17) من (ق.إ.ج.ج)[1].

5- **إبقاء الإذن بالتسرّب خارج ملف الإجراءات إلى غاية الانتهاء من العملية:** والهدف من ذلك هو الحفاظ على السرّية المطلوبة لنجاح عملية التسرّب والتي حصرها المشرع بين القاضي الآمر بها (وكيل الجمهورية أو قاضي التحقيق)، وضابط الشرطة القضائية المشرف على العملية وكذا العون المتسرّب.

6- **وجود تقرير مسبق:** يتم تحريره من طرف الضابط المسؤول عن الجريمة بشكل مفصل لاطلاع القاضي بشكل تام عن ظروف القضية ومتطلباتها وكذا جدوى عملية التسرّب، وهذا وفق نص المادة (65 مكرر13) من (ق.إ.ج.ج). وعليه يجب على الضابط المنسّق جمع أكبر قدر من المعلومات حول القضية محل التحرّي حتى يتسنى لوكيل الجمهورية أو قاضي التحقيق الأمر بإجراء عملية التسرّب أو رفضها إذا كانت تشكل خطرا على أمن العون أو ضابط الشرطة أو الاشخاص المسخرين لذلك[2].

7- **الصفة:** نستخلص من المادتين(65 مكرر12 و 65 مكرر14)على أن المخولين قانونا للعمل بنظام التسرّب هم ضباط وكذا أعوان الشرطة القضائية وكذا الأشخاص المسخرين لذلك[3].

بعد الانتهاء من عملية التسرّب، يجب إيداع رخصة التسرّب في ملف الإجراءات، وهذا وفقا لنص المادة (65 مكرر6/15) التي تنص على:"...تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرّب".

ثانيا: الشروط الموضوعية: تتمثل الشروط الموضوعية لعملية التسرّب في شرطين رئيسين هما:

1 - **التسبيب :** يعتبر التسبيب أساس العمل القضائي، وعليه يجب على وكيل الجمهورية أو قاضي التحقيق عند إصدار الإذن بالتسرّب توضيح الأدلة القانونية والموضوعية بعد تقدير جميع العناصر المعروضة عليه من طرف ضابط الشرطة القضائية، وهذا طبقا لنص المادة (65 مكرر 1/15) التي تنص على:" يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11 أعلاه، مكتوبا ومسببا وذلك تحت طائلة البطلان...".

2- **نوع الجريمة:** وقد حصرتها المادة(65 مكرر5) من (ق.إ.ج.ج) في سبعة أنواع هي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية

---

[1] المادة (65 مكرر17) من(ق.إ.ج.ج).

[2] عبد المجيد جباري، المرجع السابق، ص58.

[3] المادتان(65 مكرر12 و65 مكرر14) من (ق.إ.ج.ج).

للمعطيات، جرائم تبييض الأموال، الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، وجرائم الفساد. وعليه يجب أن تكون الجريمة جناية أو جنحة.

في هذا الشأن يُثار التساؤل الآتي: ماذا لو اكتشف المتسرّب جرائم خارج تلك المذكورة على سبيل الحصر؟. لم يتطرق المشرع إلى ذلك في أحكام التسرّب، إلا أنه بالرجوع لأحكام المادة (65 مكرر 6) من (ق.إ.ج.ج) التي تنص على:"...إذا اكتشف جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة". ورغم أن هذه المادة ذكرت في الفصل المتعلق باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، إلا أنه يمكن اعتبار الحلقة المشتركة بينها وبين أحكام التسرّب هي المادة (65 مكرر5) من (ق.إ.ج.ج) المشار إليها بالمادة(65 مكرر11) من (ق.إ.ج.ج) المتعلقة بالجرائم المطلوبة لتطبيق أحكام الأساليب الخاصة في التحقيق. وعليه يمكن القول: إن اكتشاف جريمة خارج إذن القاضي عند مباشرة عملية التسرّب، لا يمكن أن يكون سببا للبطلان، فمثلا إذا اكتشف المتسرّب بخلية لتبييض الأموال جناية قتل، يمكن له رفع تقرير بذلك إلى المشرف عليه إداريا.

ثالثا: آثار التسرّب: بعد صدور الإذن بالتسرّب من طرف وكيل الجمهورية أو قاضي التحقيق يباشر العون المتسرّب عمله حسب المقتضيات المطلوبة منه، وعليه يترتب عن ذلك آثارا نتناولها كما يأتي:

1- **تسخير الوسائل المادية والقانونية:** في هذا الصدد نصت المادة (65 مكرر 14) من (ق.إ.ج.ج) على:" يمكن ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرّب والأشخاص الذين يسخرونهم لهذا الغرض:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال".

وبالتالي يمكن للعون المتسرّب استعمال الأموال المتحصل عليها من ارتكاب الجرائم المذكورة بنص المادة (65 مكرر5) من (ق.إ.ج.ج)، ومن ثم فإن المتسرّب يمكنه تسخير الوسائل المادية لفائدة الخلية الإجرامية من النقل أو التسليم أو الحيازة ...إلخ.

أما بخصوص الوسائل القانونية فالمقصود منها توفير كافة الأدوات القانونية لمرتكبي هذه الجرائم، مثل: الحصول على الوثائق الرسمية إن كان هناك ضرورة لذلك كاستخراج بطاقة تعريف أو رخصة سياقه أو بطاقة رمادية وبالتالي يحتاج إلى جهاز خاص لتزوير الوثائق الرسمية دون المرور

على الإدارة المختصة لإبقاء أعماله ضمن السرية المطلوبة، وهذا ما يقودنا للقول بأن دور المتسرّب داخل الجماعة الاجرامية محصور بتقديم الدعم بكافة أشكاله[1].

2- **الإعفاء من المسؤولية :** بالرجوع إلى طبيعة الأفعال التي يقوم المكلف بعملية التسرّب نلاحظ أنها تستوجب العقاب، لكن نظرا لمقتضيات التحقيق في هذا الصنف من الجرائم، أدخل المشرع الجزائري نظام التسرّب ضمن أسباب الإباحة باعتبار أن القانون أذن بذلك وفقا لنص المادة (39) من (ق.ع.ج) التي تنص على: "لا جريمة إذا كان الفعل قد أمر أو أذن به القانون..."مما يجعل المتسرّب معفى من المسؤولية الجزائية وأيضا استنادا لنص المادة(65 مكرر14) من (ق.إ.ج.ج) التي تنص على :" يمكن ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرّب والأشخاص الذين يسخرونهم لهذا الغرض دون أن يكونوا مسؤولين جزائيا..." إضافة إلى نص المادة(65 مكرر 12) التي تنص على:"...يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر14 أدناه ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم". بل مدّد أيضا من نطاق هذا الإعفاء لظروف أمنية للمتسرّب حتى بعد انقضاء المهلة المحددة في رخصة التسرّب أو في حالة تقرّر وقف عملية التسرّب وفق لنص المادة(65 مكرر17) سالفة الذكر.

3- **إحاطة العملية بالسرّية التامة:** لنجاح عملية التسرّب يجب إحاطتها بالسرّية التامة لذا نص المشرع الجزائري على عقوبات مشدّدة في حالة إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية بموجب نص المادة (65 مكرر 16) من(ق.إ.ج.ج)، وقد تعدت الحماية حتى لأفراد عائلة المتسرّب وتتراوح هذه العقوبات من سنتين إلى عشرين سنة حبسا وغرامة من خمسين ألف دينار إلى مليون دينار حسب الحالات الثلاث المذكورة بالمادة[2]. وعليه يبقى العون أو الضابط المتسرّب في سرية تامة حتى أن القانون منع سماعه، وأجاز على مستوى المحاكمة سماع الضابط المشرف على العملية بوصفه شاهدا بموجب نص المادة(65 مكرر18) التي تنص على:" يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرّب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية".

---

[1] رشيدة بوكر، المرجع السابق، ص438.

[2] تنص المادة (65 مكرر16) من (ق.إ.ج.ج) على:" لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات. يعاقب كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين (2) الى خمس (5) سنوات وبغرامة من 50.000دج الى 200.000دج. وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس (5) إلى عشر (10) سنوات والغرامة من 200.000 إلى 500.000دج. وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من عشر (10) سنوات إلى عشرين (20) سنة والغرامة من 500.000دج إلى 1.000.000دج دون الاخلال عند الاقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من قانون العقوبات".

برغم أهمية إجراء التسرّب في مكافحة الجرائم المستحدثة، إلا أننا نسجل بعض الإشكالات القانونية والعملية كما يأتي[1]:

أ- **الإشكالات القانونية:** تتمثل في:

- نصت المادة (65 مكرر 14) من (ق.إ.ج.ج) على إمكانية تسخير أشخاص غير ضباط وأعوان الشرطة القضائية للقيام بعملية التسرّب، غير أنها لم تبين لنا طبيعة الأشخاص والجهة التي يسخرون من طرفها ومدى التزامهم بسرّية العملية.

- إن حصر معرفة هوية المتسرّب في ضابط الشرطة القضائية المنسق للعملية، يطرح إشكالية إيجاد حل عندما يتعرض ذلك الضابط إلى مانع يحول دون ايصال المعلومات.

- لم تسمح النصوص القانونية للتسرّب من سماع المتسرّب رغم ما يمتلكه من معلومات تفيد التحقيق، عكس المشرع الفرنسي الذي سمح للمتسرّب الإدلاء بشهادته في حالة نفي الوقائع من طرف أعضاء الشبكة الاجرامية، ويمكنه كذلك بناء على طلبه الكشف عن هويته إذا تطلب الأمر ذلك.

ب- الإشكالات العملية: تتمثل في:

- إن أغلب أعوان وضباط الشرطة القضائية معروفون لدى الأوساط الإجرامية مما ينذر بفشل عملية التسرّب وتعريض المتسرّب للخطر.

- عدم توفر الوسائل والأموال الضرورية لدى المتسرّب، والحل يكمن في إمكانية تمويل الخزينة العمومية لهذه العملية أو السماح للمتسرّب التصرف في بعض المحجوزات لضرورة العملية.

وأخيرا يهدف المشرع الجزائري من وراء استحداث هذه الأساليب الخاصة والاستثنائية في مجال البحث والتحري في جرائم التلبّس وبعض الجرائم المحددة على سبيل الحصر، ومنها الجرائم الإلكترونية رغم ما يمثل ذلك من اعتداء صارخ على حرمة الحياة الخاصة للأفراد المكفولة دستوريا إلى إظهار الحقيقة للكشف عن المجرم ومعاقبته عن طريق استخلاص الدليل الإلكتروني أو الرقمي الذي يدينه والذي تختلف طبيعته عن الدليل التقليدي، غير أننا وبصفة عامة وإضافة إلى الاشكالات القانونية والعملية السابق ذكرها نسجل النقائص التالية[2]:

- إن تحديد المشرع لفئة من الجرائم على سبيل الحصر يحد من حرية السلطة القضائية في اللّجوء إلى أساليب التحري الخاصة بسبب صعوبة وصف الجريمة وتكييفها قبل اكتمال إجراءات التحقيق، مما يؤدي إلى افلات المجرمين من العقاب في جرائم خطيرة مثل: جرائم الاختطاف والقتل بالتسميم أو تزوير النقود...إلخ.

---

[1] عبد المجيد جباري، المرجع السابق، ص ص66-67.

[2] جميلة محلق، المقال السابق، ص ص179-180.

– ربط المشرع الجزائري إجراءات التحري الخاصة بضرورة وجود فائدة منها، وعلى أساس ذلك يمنح الإذن من طرف السلطة القضائية المختصة للقيام بالإجراء المطلوب، وذلك حينما تفشل إجراءات البحث والتحري التقليدية في كشف الحقيقة، كما تبرّر بمدى تحقيق التوازن بين المصلحة العامة والمصلحة الخاصة، مصلحة الدولة في فاعلية العدالة الجنائية في ملاحقة المجرم وتوقيع العقاب عليه، ومصلحة الفرد في عدم انتهاك حرمة حياته الخاصة. خاصة ما تعلق بالبحث والتحري عن الجرائم الإلكترونية.

كما تجدر الإشارة إلى أنه ونظرا للصعوبات البالغة التي تواجهها الضبطية القضائية في مجال البحث والتحري وجمع الأدلة في مجال الجرائم الإلكترونية بسبب طبيعتها الخاصة، أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بالجزائر العاصمة، إضافة إلى مَخبرين جهويين بكل من قسنطينة ووهران يحتوي كل منهما على خلية للإعلام الآلي. من جهة أخرى تم تدعيم مراكز الأمن الولائي بفرق متخصّصة بالتحقيق في مجال الجرائم الإلكترونية تعمل بالتنسيق مع المخابر المركزية. والأمر نفسه قامت به القيادة العامة للدرك الوطني، حيث أنشأت قسم الإعلام والإلكترونيك يختص بالتحقيق في الجرائم الإلكترونية، إضافة إلى إنشاء المركز الوطني للوقاية من الجرائم المعلوماتية ومقرّه بالجزائر العاصمة.

من جانب آخر، تثير مسألة الاختصاص القضائي للسلطات القضائية المكلفة بالتحريات والتحقيقات إشكالات عديدة نظرا للطبيعة الخاصة للجرائم الإلكترونية، إضافة إلى إمكانية مساس إجراءات الحصول على الأدلة الرقمية بخصوصية الفرد المكفولة دستوريا. فكيف عالج المشرع الجزائري في إطار سياسته الجنائية الإجرائية هذه الاشكالات بما يخدم مصلحة المجتمع والفرد غلى حد سواء؟ هذا ما سنتناوله في المطلب الموالي.

المطلب الرابع: الاختصاص القضائي في الجرائم الإلكترونية

إن موضوع الاختصاص القضائي في الجريمة الإلكترونية، وفي ظل الطبيعة الخاصة لهذه الأخيرة التي تتم في بيئة افتراضية لا تعترف بالحدود الجغرافية، يُثير مسألة تنازع الاختصاص المحلي بين أكثر من جهة قضائية داخل الدولة. إن الأمر لا يقتصر على المشكلات الإجرائية التي تخص ضبط الجريمة وإثباتها –كما رأينا سابقا– فحسب، بل نجد أنفسنا أمام مشكلة أكثرُ تعقيداً تتمثل في تحديد الاختصاص القضائي للجهات القضائية المكلفة بالتحريات والتحقيقات، فقواعد الاختصاص القضائي التقليدية صيغت لكي تحدد الاختصاص المتعلق بجرائم قابلة للتحديد المكاني للجريمة. فكيف تعامل المشرع الجزائري بشأن توزيع الاختصاص القضائي بين سلطات البحث والتحري في مجال مكافحة الجرائم الإلكترونية؟.

سنتناول الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق في (الفرع الأول)، ثم نتطرق إلى الصلاحيات المكانية للضبطية القضائية في الجرائم الإلكترونية في(الفرع الثاني).

الفرع الأول: الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق:

يقوم هذا النوع من الاختصاص بتحديد إطار جغرافي بمنطقة معينة من إقليم الدولة، حيث يعتمد معايير ثلاثة: مكان وقوع الجريمة، أو مكان إقامة المتهم، أو مكان القبض على المتهم.

أولا: الاختصاص المحلي لوكيل الجمهورية : تتعدد الجهات القضائية على مستوى إقليم الدولة الواحدة، وتختلف بذلك المهام التي أسندها المشرع لكل جهة قضائية على حدة، حسب درجتها وحسب نوع القضايا التي يُوكل لها مهام الفصل فيها، وحسب نطاقها الإقليمي الذي تمارس اختصاصها فيه.

يتحدد الاختصاص المحلي لوكيل الجمهورية طبقا لنص المادة (1/37) من (ق.إ.ج.ج) التي تنص على:" يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر...". وعليه يمكن القول أنه يتحقق اختصاص وكيل الجمهورية بتوافر الشروط الآتية:

- أن تكون الجريمة قد اقترفت في دائرة اختصاص وكيل الجمهورية المكاني.
- أن تكون إقامة أحد المشتبه في ارتكابهم الجريمة بنفس دائرة الاختصاص.
- أن يكون قد ألقي القبض على أي من المشتبه فيهم في تلك الدائرة. ولو تمّ القبض لسبب آخر.

• **تمديد الاختصاص لوكيل الجمهورية:** نظرا لخطورة وطبيعة بعض الجرائم ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، نص المشرع الجزائري على تمديد الاختصاص المحلي لوكيل الجمهورية ليشمل كافة الإقليم الوطني وذلك بنص المادة (2/37) من (ق.إ.ج.ج) التي تنص على:"...يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف"[1].

---

[1] عُدلت المادة (37) بالقانون رقم:04-14 المؤرخ في:2004/11/10، المعدل والمتمم لقانون الإجراءات الجزائية (ج. ر) رقم: 71 المؤرخة في: 2004/11/10، ص5 .

وعليه أصدر المشرع الجزائري المرسوم التنفيذي رقم:06-348 المؤرخ في:2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، أين وزّعت المواد من (05-02) منه الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق حسب الجدول الآتي[1]:

إسم المحكمة التي يمتد اختصاصها إلى محاكم أخرى(محكمة القطب)	أسماء محاكم المجالس القضائية التابعة لمحكمة القطب	ملاحظة
1- محكمة سيدي محمد بالجزائر العاصمة:	الجزائر -الشلف-الأغواط-البليدة-البويرة-تيزي وزو -الجلفة-المدية-المسيلة-بومرداس-تيبازة-عين الدفلى	
2- محكمة قسنطينة:	قسنطينة-أم البواقي-باتنة-بجاية-بسكرة-تبسة-جيجل-سطيف-سكيكدة-عنابة-قالمة-برج بوعريريج-الطارف-الوادي-خنشلة-سوق أهراس-ميلة	
3- محكمة ورقلة:	ورقلة-أدرار - تامنغست-إيليزي-تندوف-غرداية	
4- محكمة وهران:	وهران-بشار -تلمسان-تيارت-سعيدة-سيدي بلعباس-مستغانم-معسكر -البيض-تيسمسيلت-النعامة-عين تموشنت-غليزان.	

تجدر الإشارة إلى أن المحاكم التي تم تمديد اختصاصها اصطلح على تسميتها بالأقطاب الجزائية أو محكمة القطب. وبذلك تجاوز المشرع الجزائري في سياسته الجنائية الإجرائية مشكلة هامة إذ يمكن بهذا الإجراء تسهيل عمل الأجهزة القضائية المكلفة بالتحريات والتحقيقات في إطار مكافحة الجريمة الإلكترونية، على اعتبار الطبيعة الخاصة لهذا النوع من الجرائم الذي يتم في عالم افتراضي لا حدود له.

[1] المواد (05-02) من المرسوم التنفيذي رقم:06-348 المؤرخ في:2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، (ج.ر) رقم:63 المؤرخة في:2006/10/08، ص30.

وتحسبا لما قد يطرأ من إشكالات إثر تطبيق هذا المرسوم، خولت المادة (6) منه إلى رئيس المجلس القضائي الذي تقع في دائرة اختصاصه المحكمة التي تم تمديد اختصاصها بمعنى: رؤساء المجالس القضائية لكل من مجلس قضاء الجزائر وقسنطينة وورقلة ووهران[1].

من جهة أخرى وسّع المشرع الجزائري من الاختصاص المحلي للنيابة العامة في مجال تتبع الجرائم الإلكترونية، وأجبرها بأن تباشر إجراءات المتابعة الجزائية تلقائيا، وذلك في المواد(144 مكرر -144 مكرر2) من (ق.ع.ج) والمتعلقة بجرائم القذف باستعمال أي وسيلة إلكترونية أو معلوماتية سواء في حق رئيس الجمهورية أو الرسول صلى الله عليه وسلم أو الأنبياء وكذا المعلوم من الدين بالضرورة...إلخ [2].

من المعلوم أن وكيل الجمهورية وعند إخطاره من قبل الضبطية القضائية بإحدى الجرائم المنصوص عليها بموجب المادة (2/37) من (ق.إ.ج.ج) مثل: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، بواسطة أصل ونسختين من ملف إجراءات التحقيق وفقا لنص المادة(40 مكرر1) من (ق.إ.ج.ج)، يُرسل النسخة الثانية فورا للنائب العام لدى المجلس القضائي التابعة له المحكمة ذات الاختصاص الموسّع وذلك طبقا للسلم الإداري، ولهذا الأخير أن يطلب موافاته بالإجراءات إذا ما تبين له أن الجريمة تندرج ضمن اختصاص محكمة القطب، وانطلاقا من هذه اللحظة وبعد أن تمسك هذه الجهة باختصاصها فإن ضباط الشرطة القضائية الذين أنجزوا الملف يتلقون تعليماتهم مباشرة من وكيل الجمهورية للمحكمة ذات الاختصاص الموسع[3].

ثانيا: الاختصاص المحلي لقاضي التحقيق: حددت المادة (1/40) من (ق.إ.ج.ج) الاختصاص المحلي لقاضي التحقيق بقولها :" يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر". وعليه يمكن القول أنه لتحقق الاختصاص المحلي لقاضي التحقيق يجب توفر الشروط الآتية:

- أن تكون الجريمة قد اقترفت في دائرة اختصاص قاضي التحقيق المكاني.
- أن تكون إقامة أحد المشتبه في ارتكابهم الجريمة بنفس دائرة الاختصاص.
- أن يكون قد ألقي القبض على أي من المشتبه فيهم في تلك الدائرة.

1 المرجع نفسه، المادة (06) .

2 المادتان (144مكرر) و(144مكرر2) من (ق.ع.ج).

3 عبد المجيد جباري، المرجع السابق، ص119.

• **تمديد الاختصاص لقاضي التحقيق:** ومثلما فعل المشرع مع تمديد الاختصاص لوكيل الجمهورية وللأسباب نفسها، نص على تمديد الاختصاص المحلي لقاضي التحقيق ليشمل كافة الإقليم الوطني وذلك بنص المادة (2/40) من (ق.إ.ج.ج) التي تنص على:"...يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف"[1]. كما نشير أيضا إلى أن تمديد الاختصاص المحلي لقاضي التحقيق مشمولا كما هو الشأن بالنسبة لوكيل الجمهورية بأحكام المرسوم التنفيذي رقم: 06-348 المؤرخ في:2006/10/05 سالف الذكر.

من ناحية أخرى نصت المادة (3/47) من (ق.إ.ج.ج) على:"...وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص...". كما نص أيضا بموجب المادة (4/47) على:" عندما يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، يمكن قاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك".

في المجال نفسه، نصت المادة (4/329) من (ق.إ.ج.ج) على تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف"[2]، كما نلاحظ أيضا أن المشرع الجزائري لم يقتصر على تمديد الاختصاص القضائي في مفهومه التقليدي المادي، بل تجاوز ذلك إلى تمديد الاختصاص في العالم الافتراضي وذلك حينما يتعلق الأمر بتفتيش المنظومة المعلوماتية عن بعد، حيث نصت المادة (5) من القانون 09-04 السابق ذكره على:" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه، الدخول بغرض التفتيش ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

---

[1] عُدلت المادة (40) بالقانون رقم:04-14 المعدل والمتمم.

[2] عُدلت المادة (329) بالقانون رقم:04-14 المعدل والمتمم.

ب- منظومة تخزين معلوماتية...".

فمن خلال هذه المادة أجاز المشرع الدخول بغرض التفتيش ولو عن بعد إلى المنظومة المعلوماتية ودون إذن صاحبها.

الفرع الثاني: الصلاحيات المكانية للضبطية القضائية في الجرائم الإلكترونية:

غالبا ما تبدأ الإجراءات الجزائية في الدعوى العمومية بمرحلة البحث والتحري أو مرحلة جمع الاستدلالات التي تتولاها أصلا الضبطية أو الشرطة القضائية، ولقد حدّد (ق.ا.ج.ج) أحكام الضبط القضائي في المواد من:(12 إلى 28 و42 إلى 55 و63 إلى 65)، وتشمل الضبطية القضائية ضباط الشرطة القضائية وأعوانهم وبعض الموظفين المنوطة بهم بعض مهام الشرطة القضائية. عند انتهاء ضابط الشرطة القضائية من مهمته يرسل محاضر البحث الأولى إلى وكيل الجمهورية الذي له حق التصرف فيها. وعليه يطرح التساؤل الآتي: هل نص المشرع الجزائري على تمديد اختصاصات ضباط الشرطة القضائية بخصوص الجرائم الإلكترونية مثلما فعل مع وكيل الجمهورية وقاضي التحقيق؟.

تنفيذا للسياسة الإجرائية للمشرع الجزائري بخصوص مكافحة الجرائم الإلكترونية خاصة في مجال البحث والتحري، أجازت المادة (7/16) تمديد اختصاصات ضباط الشرطة القضائية في حالة البحث والمعاينة إلى كافة الإقليم الوطني، مثلما فعل المشرع مع وكيل الجمهورية وقاضي التحقيق حيث تنص على:" غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد اختصاص ضباط الشرطة القضائية إلى كافة الإقليم الوطني. ويعمل هؤلاء تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات".

كما يلتصق بمهام الضبط القضائي أعمال المعاونة والمساعدة[1] المنوطة بأعوان الضبط القضائي الذين تبينهم المادة (19) من (ق.إ.ج.ج)[2]، ويلحق بهم أيضا سلطات الولاة في مجال الضبط القضائي والمحددة في حالة وقوع جناية أو جنحة ضد أمن الدولة.

---

[1] حيث تنص المادة (20) من (ق.إ.ج.ج) على:" يقوم أعوان الضبط القضائي الذين ليست لهم صفة ضابط الشرطة القضائية بمعاونة ضباط الشرطة القضائية في مباشرة وظائفهم ويثبتون الجرائم المقررة في قانون العقوبات ممتثلين في ذلك لأوامر رؤسائهم مع الخضوع لنظام الهيئة التي ينتمون إليها ويقومون بجمع كافة المعلومات الكاشفة عن مرتكبي تلك الجرائم".

[2] تنص المادة (19) من (ق.إ.ج.ج) على: "يعد من أعوان الضبط القضائي موظفو مصالح الشرطة وذوو الرتب في الدرك الوطني ورجال الدرك ومستخدمو مصالح الأمن العسكري الذين ليست لهم صفة ضباط الشرطة القضائية".

من جهة أخرى، يمكن لضباط الشرطة القضائية وأعوان الشرطة القضائية في حال عدم اعتراض وكيل الجمهورية، تمديد عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرّر يحمل على الاشتباه فيهم بارتكاب جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، وهذا بموجب نص المادة (16مكرر) من (ق.إ.ج.ج) التي تنص على:" يمكن ضباط الشرطة القضائية، وتحت سلطتهم أعوان الشرطة القضائية، ما لم يعترض على ذلك وكيل الجمهورية المختص بعد إخباره، أن يمددوا عبر كامل الإقليم الوطني عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الاشتباه فيهم بارتكاب الجرائم المبينة في المادة (16) أعلاه أو مراقبة وجهة أو نقل أشياء أو أموال أو متحصلات من ارتكاب هذه الجرائم أو قد تستعمل في ارتكابها". وبهذا الإجراء يمكن ملاحقة المجرم الإلكتروني عن طريق مراقبته عبر كامل التراب الوطني خاصة في حالة تشكيل جمعية أشرار.

إن هدف المشرع الجزائري من استحداث أساليب بحث وتحري تتلائم وطبيعة الجرائم المستحدثة ومنها الجرائم الإلكترونية، هو استخلاص الأدلة الرقمية التي يمكن من خلالها إدانة المجرم المعلوماتي. لكن بالمقابل تظهر مسألة جديدة في غاية الأهمية، حيث يُثار التساؤل الآتي: ما مدى حجية الدليل الإلكتروني في الإثبات الجنائي؟ هذا ما سنتناوله في المبحث الثالث.

المبحث الثالث: حجية الدليل الإلكتروني في الإثبات الجنائي

أدى سوء استخدام الفضاء السبراني إلى بروز جرائم مستحدثة، تطلبت نوعا جديدا من الأدلة تسمى بالأدلة الرقمية، أو الأدلة الإلكترونية، تتفق وطبيعة الوسط الافتراضي الذي ارتكبت فيه الجريمة. فكان التحدّي أمام المشرع الجزائري ليس فقط تحديد هذه الأفعال بدقة، ولكن إيجاد حلول للمشكلات المتعلقة بالدليل الإلكتروني من حيث الوسائل المستعملة في ذلك، وإجراءات الحصول عليه، إضافة إلى مدى تأثير مشكلات الدليل الإلكتروني على مبدأ اقتناع القاضي وسلطته في تقدير الدليل الرقمي...إلخ.

سنتناول ماهية الدليل الإلكتروني في (المطلب الأول)، ثم نتطرق إلى مدى حجية الدليل الإلكتروني في ظل أنظمة الإثبات المختلفة في (المطلب الثاني)، ثم نتناول سلطة القاضي الجنائي في تقدير الدليل الإلكتروني في (المطلب الثالث)، لنتطرق في الأخير إلى مدى تأثير مشكلات الدليل الإلكتروني على مبدإ اقتناع القاضي في (المطلب الرابع).

المطلب الأول: ماهية الدليل الإلكتروني

بالرجوع إلى معنى الإثبات، فهو "يعني إقامة الدليل أمام القضاء بالطرق القانونية التي حددها القانون على وجود واقعة ترتب آثارها"[1]، ومن القواعد المستقرة في مجال الإثبات الجنائي أن القاضي لا يمكنه أن يقضي بعلمه الشخصي، فإحاطته بوقائع الدعوى يجب أن يتم من خلال ما يطرح عليه من أدلة وعلى أساسه يبني قناعته، وكما عرفنا سلفا أن الجريمة الإلكترونية ذات طبيعة خاصة ينتج عنها أيضا أن الدليل المستخلص منها، يكون ذا طبيعة خاصة مما يخلق صعوبات للمشرع ولأجهزة البحث والتحري على حد سواء، في مجال تحديد طبيعته وحجيته وطرق استخلاصه.

سنتناول مفهوم الدليل الإلكتروني في (الفرع الأول)، ثم نتطرق إلى طبيعته الخاصة في (الفرع الثاني).

الفرع الأول: مفهوم الدليل الإلكتروني:

يعتبر الدليل عموما وسيلة يمارس من خلاله القاضي سلطته التقديرية في إصدار أحكامه، كما تختلف السلطة التقديرية للقاضي باختلاف نظم الإثبات الجنائي حيث إن للقاضي دورا إيجابيا في نظام الإثبات المعنوي، ودورا سلبيا في نظام الإثبات القانوني[2]. ولهذه الأهمية التي يتمتع بها الدليل عموما حظي باهتمام المشرع في مختلف الأنظمة القانونية من حيث تحديد شروط مشروعيته وتقدير قيمته الإثباتية. إن البحث في مسألة الإثبات بالأدلة الرقمية، يبدو غير ذي معنى إذا لم يكن مدعما من قبل التقنية ذاتها[3]، ومما لا شك فيه أن الثورة العلمية في مجال نظم المعلومات الإلكترونية، لم تؤثّر فقط في نوعية الجرائم التي ترتبت عليها من حيث مرتكبيها أو محلها أو وسائلها، وإنما أثرت أيضا على طرق الإثبات، بحيث صارت طرق الإثبات التقليدية عقيمة في مواجهة هذه الجرائم وبالتالي إفلات المجرم من العقاب، مما أدى إلى ظهور الدليل الإلكتروني أو الرقمي[4]. كما أن إثبات الجرائم الإلكترونية يكمن في صعوبة كشف الجاني في ظل هذا الفضاء الافتراضي اللاّمتناهي[5]، مما يتطلب استخدام وسائل إلكترونية تتلائم وطبيعة هذه الجرائم لكشفها في زمن ارتكابها، وإن تعذر إقامة الدليل اللاّزم لإثباتها سيترتب عنه إلحاق الضرر بالأفراد وبالمجتمع.

---

[1] كوثر أحمد خالند، الإثبات الجنائي بالوسائل العلمية، دراسة تحليلية مقارنة، دار التفسير للنشر والإعلان، العراق، ط1، 2007 ص30.

[2] زيدان فاضل، سلطة القاضي الجنائي في تقدير الأدلة، دار الثقافة للنشر والتوزيع، عمان، الأردن،1999، ص144.

[3] محمد فتحي محمد أنور عزت، المرجع السابق، ص403.

[4] يرجع أصل استخدام الدليل الرقمي إلى استخدام النظام الثنائي الرقمي *(binary)* الذي اعتمد أساسا لعمل الكمبيوتر، فهو لا يستعمل إلا الرقمين(0) و (1)، أي يعتمد الأساس(2)، ومن خلاله يمكن تحويل الأرقام العشرية والحروف والأشكال والصور إلى نظام ثنائي، كما يوجد هناك أنظمة أخرى، كالنظام العددي العشري، إذ يمكن دمج هذه الأنظمة مع بعضها، وغالبا ما يتم ذلك في مراحل مختلفة من الإجراءات على الحاسوب، راجع، محمد أمين فكيرين، أساسيات الحاسب الآلي، دار الراتب الجامعية، بيروت، لبنان،1993، ص ص35-36.

[5] *CHRISTIANE FERAL-SCHUHL, Le Droit à L'épreuve , Quatrième édition , Op.Cit,p.602.*

ونظرا لحداثة وأهمية الدليل الإلكتروني، تعددت التعريفات واختلفت بخصوص وضع تعريف له سنتطرق إلى أهمها:

فقد عرفه البعض على أنه:" تلك الأدلة التي يمكن الحصول عليها بإحدى وسائل الإخراج"[(1)] أو هو:" الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، وهو مكوّن رقمي لتقديم معلومات في أشكال متنوعة مثل: النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ القانون"[(2)]. وعرفه آخرون على أنه: "الدليل الذي يجد لها أساسا في العالم الافتراضي ويقود إلى الجريمة"، كما عرفه فريق عمل المنظمة الدولية لأدلة الحاسوب على أنه:" المعلومات المخزنة أو المتنقلة في شكل ثنائي، ذات قيمة إثباتية"[(3)].

لقد حصرت هذه التعاريف مفهوم الدليل الرقمي في الذي يتم استخراجه من الحاسوب فقط ولاشك أن ذلك فيه تضييق لدائرة الأدلة الرقمية، إذ يمكن الحصول عليها من أية آلة رقمية أخرى كالهاتف الذكي وآلات التصوير وغيرها من الأجهزة التي تعتمد التقنية الرقمية في تشغيلها، فضلاً عن ذلك فإن هذا التعريف يخلط بين الدليل الرقمي ومصدر استخلاصه، حيث عرَّفه بأنه الدليل المأخوذ من الحاسوب، وهذا يعني أن الدليل الرقمي لا تثبت له هذه الصفة إلا إذا تم استخلاصه من مصدره وهذا ليس صحيحاً، حيث يقودنا هذا للقول بأن المجالات المغناطيسية أو الكهربائية قبل فصلها عن مصدرها بواسطة الوسائل الفنية لا تصلح لأن توصف بالدليل الرقمي، أي أن مخرجات الآلة الرقمية لا تكون لها قيمة إثباتية مادامت في الوسط الافتراضي الذي نشأت فيه أو بواسطته[(4)].

من خلال ما سبق يمكن استخلاص تعريف للدليل الرقمي على أنه: معلومات مخزنة في نظام المعالجة الآلية وملحقاتها مثل: الأقراص الصلبة والمرنة والطابعة...إلخ، أو متنقلة عبر شبكات الاتصال، تكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة لتظهر في شكل مخرجات ورقية أو إلكترونية أو معروضة على شاشة أو غيرها لإثبات وقوع الجريمة ونسبتها لفاعلها.

إن الدليل الإلكتروني ليس على صورة واحدة، ويمكن تقسيمه إلى ثلاثة أقسام:

---

[1] سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي-دراسة مقارنة، دار الكتب القانونية مصر،2011، ص55.

[2] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006 ص77.

[3] طارق فوزي الفقي، الجوانب الإجرائية في الجرائم المعلوماتية-دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنوفية، مصر 2011، ص80.

[4] رشيدة بوكر، المرجع السابق، ص385.

- **القسم الأول: المخرجات الورقية:** والتي يمكن استخراجها من الحاسوب بواسطة الآلة الطابعة، حيث تتنوع هذه الطابعات من حيث طريقة وسرعة تشغيلها وخصائص المخرجات الورقية[1].

- **القسم الثاني: المخرجات اللاّورقية أو الإلكترونية:** حيث يقوم المستخدم بإدخال البيانات والحصول على المخرجات في الوقت نفسه، حيث يمكن تثبيتها على دعامات مثل: الأشرطة المغناطيسية، والأقراص الصلبة أو المرنة والأقراص المضغوطة والمدمجة، والذاكرة الوميضية...إلخ[2].

- **القسم الثالث: مخرجات العرض المرئي:** والتي تعرض على شاشات الحاسوب وهي من أهم أجزاء الحاسوب إذ يتم بواسطتها عرض أي بيانات أو معلومات تكتب على لوحة المفاتيح بواسطة المستخدم، كما يتم استعراض البيانات المدخلة أو المعلومات الناتجة عن معالجة المعطيات في وحدة المعالجة المركزية *(Central Processing Unit)*، وكذلك التعليمات الموجهة للمستخدم عن طريق البرامج التطبيقية[3].

الفرع الثاني: الطبيعة الخاصة للدليل الإلكتروني:

تعتبر قاعدة جواز الإثبات بكافة طرق الإثبات القانونية في الدعاوى الجزائية من القواعد الأساسية التي تضمن حق المتهم في الدفاع عن نفسه، والقيد على هذه القاعدة أن الدليل يتعين أن يكون من الأدلة التي يقبلها القانون، وبالتالي تظهر أهمية اعتراف القانون بالأدلة ذات الطبيعة الإلكترونية، خاصة مع ظهور أنشطة إجرامية عديدة في بيئة الأعمال والتجارة والبنوك الإلكترونية والمعلومات...إلخ. من هنا اتجه المشرع في العديد من الدول إلى الاعتراف بالحجية القانونية لملفات الحاسوب ومستخرجاته والرسائل الإلكترونية ذات المحتوى المعلوماتي ضمانا لعدم إفلات المجرم الإلكتروني من العقاب. كما تجدر الإشارة إلى أن تأثير التطور العلمي لا يقف عند مضمون الدليل وطبيعته الخاصة، وإنما يمتد هذا التأثير كذلك إلى الإجراءات التي يترتب عليها الحصول على هذا الدليل، ولذلك فإنه يجب أن تكون هذه الإجراءات الجديدة ذات طبيعة خاصة ومشروعة لكي تحافظ على شرعية الأدلة المتولدة منها.

إن الجرائم التي ترتكب بالوسائل الإلكترونية في صورها الغالبة، قد تقع بسبب الغش أو التزوير أو التعديل أو المحو...إلخ في البيانات المعالجة آليا، سواء تمت هذه الأفعال أثناء إدخال هذه البيانات أو أثناء تخزينها أو أثناء إخراجها. ولذلك فإن الوصول إلى هذه الأفعال يحتاج إلى أدلة

---

[1] سامي جلال فقي حسين، الأدلة المتحصلة، المرجع السابق، ص ص55-63.

[2] ضياء على أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، مجلة سلسلة الدراسات القانونية في المجال المعلوماتي، مطبعة دور الوراقة الوطنية، المملكة المغربية، العدد 1، 2011، ص ص285-286.

[3] سامي جلال فقي حسين، الأدلة المتحصلة، المرجع السابق ، ص ص55-63.

علمية وفنية يمكنها أن تثبت وقوعها وتسندها إلى الأشخاص المتهمين بارتكابها، وهي وظيفة الدليل الرقمي، وعليه تتجلى الطبيعة الخاصة للدليل الإلكتروني في الخصائص الآتية:

أولا: دليل علمي غير مرئي: يعتبر الدليل الرقمي من الأدلة الفنية العلمية، فلا يجب أن يتعارض مع القاعدة العلمية السليمة وإلا فقد معناه[1]، فهو يتعلق بجريمة ترتكب عن طريق الحاسوب أو شبكة الإنترنت، فيمكن للمجرم المعلوماتي عن طريق نبضات إلكترونية غير مرئية العبث في بيانات الحاسوب أو برامجه في وقت قياسي، يؤدي إلى محو أو تعديل أو تغيير الدليل الرقمي باستعمال برامج ووسائل عديدة مثل: شبكات *(Botnet)* و*(Keylogger)* قبل أن تصل يد العدالة إليه خاصة ما تتطلبه عملية الضبط من إجراءات وأجهزة خاصة في مجال مكافحة الجرائم الإلكترونية[2].

وعليه يتكون الدليل الرقمي من بيانات ومعلومات في شكل إلكتروني غير ملموس لا يدرك بالحواس العادية، فهي بيانات غير مرئية لا تفصح عن شخصية معينة وهذه البيانات مسجلة إلكترونيا بكثافة، وبصورة مرمزة غالبا ما تكون على دعائم أو وسائط تخزين، حيث يتطلب إدراكها الاستعانة بأجهزة ومعدات حاسوبية واستخدام نظم وبرامج[3]. يعني هذا أنه كدليل تقني ينتمي لبيئة تقنية المعلومات يحتاج إلى هذه البيئة الخاصة حتى ينتج آثاره، وبالتالي فإن الطبيعة غير المرئية للدليل الإلكتروني تخلق مشكلات جمة للجهات المعنية خاصة ما تعلق بفحصها واستخراجها وتحليلها، إذ نحتاج إلى إجراءات خاصة تتناسب وطبيعتها الإلكترونية، تجنبا لقطع الصلة بين المجرم وجريمته[4].

ثانيا: فقدان الآثار التقليدية للجريمة : إن الجرائم الإلكترونية ليست كالجرائم التقليدية، فهي لا تخلّف آثارا مادية ويرجع السبب في ذلك إلى أن بعض العمليات يتم إدخال بياناتها مباشرة في جهاز الكمبيوتر دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها، كما لو كان البرنامج معدا ومخزنا على الحاسوب، حيث يقوم المجرم الإلكتروني بارتكاب جرائم عديدة كجرائم المساس بأنظمة المعالجة الآلية للمعطيات...إلخ، وذلك بإدخال بيانات غير مطلوبة أو تعديل البرنامج المخزن في جهاز الكومبيوتر. حيث تكون النتيجة مخرجات وهمية دون استخدام وثائق أو مستندات ورقية وبالتالي تفقد الجريمة آثارها التقليدية[5]. ومن الأسباب أيضا امتلاك الجاني لوسائل تمكنه من محو

---

[1] ضياء على أحمد نعمان، المقال السابق، ص293.

[2] *Ali EL AZZOUZI, Op.Cit,pp.60-66.*

[3] طارق فوزي الفقي، الرسالة السابقة، ص85.

[4] فؤاد حسن العزيزي، المرجع السابق، ص191.

[5] نادية سحتوت، التنظيم القانوني للجريمة المعلوماتية-أدلة اثبات الجريمة المعلوماتية، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 1، 2009، ص10.

وإتلاف آثار جريمته، وبالتالي تدمير أدلة إدانته مما يُصعّب من عمل الأجهزة المختصة لملاحقته وقد يفلت في كثير من الأحيان من العقاب[1].

ثالثا: صعوبة التخلّص من الدليل الإلكتروني: وهذه الخاصية يتميز بها عن غيره من الأدلة التقليدية، بحيث يمكن التخلص وبكل سهولة من بعض الأدلة التقليدية كالأوراق والأشرطة المسجلة بإتلافها وحرقها، كما يمكن التخلص من بصمات الأصابع بمسحها أو تهديد الشهود لثنيهم عن الشهادة أو حتى قتلهم إن تطلب الأمر. لكن يختلف الأمر بالنسبة للدليل الإلكتروني، حيث تتيح تقنية المعلومات استرجاع المعلومات بعد محوها أو إتلافها باستعمال خاصية *(Erase,Remove,delete…)*[2]، ورغم ذلك يمكن استرجاعها باستعمال برامج حاسوبية متطورة مثل: برنامج *(Recover Lost Data)*، سواء كانت هذه البيانات صورا أو رسوما أو كتابات...إلخ إذ تشكل هذه الخاصيّة صعوبة للمجرم في إخفاء جريمته، خاصة إذا تم الإبلاغ عنها للجهات القضائية في الوقت المناسب[3].

رابعا: القابلية للنسخ: تتيح التقنية المعلوماتية استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها القيمة العلمية نفسها، وهذه الخاصية لا تتوافر في الأدلة الجنائية التقليدية، مما يشكل ضمانة فعّالة لعدم إتلاف الدليل أو فقده أو تلفه[4]، حيث يمكن نسخ البيانات على دعامة إلكترونية تمهيدا لحجزها وتقديم أمام القضاء، حيث أجاز المشرع الجزائري نسخ وإفراغ المعطيات على دعامة تخزين إلكترونية تكون قابلة للحجز مثل: القرص الصلب أو المضغوط أو الذاكرة الوميضية...إلخ وهذا بموجب نص المادة (6) من القانون 09-04 سالف الذكر، وهو ما سنتطرق إليه لاحقا بخصوص الإجراء المتعلق بتفتيش وحجز المعطيات.

خامسا: الطبيعة الديناميكية والمتطورة للدليل الإلكتروني: توفر تقنية الحوسبة والاتصال سرعة هائلة في انتقال المعلومات عبر شبكات الاتصال، كما أن الدليل الإلكتروني متطور بطبيعته ولا يتصف بالجمود تبعا للتطور المتلاحق في مجال ثورة المعلومات[5]، فبيئة الدليل الرقمي من بيئة الجريمة الإلكترونية التي تقع في عالم افتراضي لا حدود فيه، حيث تنتج التقنية نبضات رقمية ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعديّة لحدود الزمان

---

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي، المرجع السابق، ص45.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص185.

[3] طارق فوزي الفقي، الرسالة السابقة، ص86.

[4] عائشة بن قارة، المرجع السابق، ص64.

[5] ضياء على أحمد نعمان، المقال السابق، ص295.

والمكان[1]. حيث تنعكس الطبيعة المتطورة للدليل الرقمي على الطرق والأدوات التقنية المستخدمة في جمع الأدلة الإلكترونية، إذ تستعمل برامج متعددة ومتطورة لهذا الغرض توفرها تقنية المعلومات[2].

من جهة أخرى، أدى تميّز الأدلة الرقمية عن الأدلة التقليدية في التحقيق الجنائي، إلى إنشاء الولايات المتحدة الأمريكية "المنظمة الدولية لأدلة الحاسوب" *(IOCE)* ، كما تم إصدار "المجلة الدولية للأدلة الرقمية" *(IJDE)*، من أجل توحيد الجهود في مجال تقنيات جمع واستخلاص وحفظ الأدلة الرقمية[3].

بعدما عرفنا الطبيعة الخاصة للدليل الإلكتروني، فهي تثير مسألة حجيته أمام القضاء، فلأي مدى يُؤخذ به؟.

المطلب الثاني: مدى قبول الأنظمة القضائية بحجية الدليل الإلكتروني في الإثبات الجنائي

يعرف الإثبات الجنائي على أنه:" إقامة الدليل لدى السلطات المختصة بالإجراءات الجنائية على حقيقة واقعة ذات أهمية قانونية بتلك الطرق التي حددها القانون وفق القواعد التي أخضعها لها"[4]. إذن فالإثبات أو الحجية تعني الاستدلال على صدق الدعوى أو كذبها، وهي تعني البينة أيضا[5]، فإن حجية المخرجات الإلكترونية بأنواعها المختلفة هي قوتها الثبوتية من حيث إسناد الفعل المُجرّم للمتهم من عدمه. إن المعلومات المستخلصة من الأدلة الرقمية كثيرة ومتنوعة مثل: صفحات المواقع الإلكترونية، والبريد الإلكتروني، ومواقع التواصل الاجتماعي*(facebook,twitter,instagram...)*، والملفات المخزنة في الحاسوب، والدخول للخدمة والاتصال بشبكة المعلومات...إلخ، لا تزال تثير خلافا حول مدى حجيتها في الإثبات بحسب اختلاف نظم الإثبات سواء كان في نظام الإثبات الحر، أو في نظام الإثبات المقيد، أو في نظام الإثبات المختلط[6]، ناهيك عن مشكلات أخرى أثيرت أيضا، مثل: اعتماد بروتوكول *(TCP/IP)*[1] كدليل

---

1 طارق فوزي الفقي، الرسالة السابقة، ص86.

2 توفر تقنية المعلومات برامج متنوعة لجمع الأدلة الرقمية مثل: برنامج إذن التفتيش- قرص بدء تشغيل الحاسوب- برنامج معالجة الملفات- برنامج النسخ-برنامج كشف الديسك- برنامج الاتصالات...إلخ، أكثر تفاصيل راجع، خالد ممدوح إبراهيم، الجرائم المعلوماتية المرجع السابق، ص203، وأيضا، حسن طاهر داود، الحاسب وأمن المعلومات، المرجع السابق، ص228، وضياء على أحمد نعمان المقال السابق، ص ص297-298، وأيضا، عادل عزام سقف الحيط، المرجع السابق، ص ص245-249.

3 طارق فوزي الفقي، الرسالة السابقة، ص92.

4 سامي جلال فقي حسين، الأدلة المتحصلة، المرجع السابق، ص67.

5 نصرالدين مروك، محاضرات في الإثبات الجنائي، درا هومة ، الجزائر، ج2، 2004، ص461.

6 يقصد بـ:

- نظام الإثبات الحر: هو ذلك النظام الذي لا يحدد طرقا معينة للإثبات، وإنما يترك لأطراف الدعوى تقديم أدلتهم ليقوم القاضي الجنائي في الأخير بتقييمها والتوصل لقناعة معينة لإصدار حكمه.

رقمي له حجية، سنتطرق إلى حجية الدليل الإلكتروني في ظل أنظمة الإثبات المختلفة في (الفرع الأول) ثم نتناول موقف المشرع الجزائري من حجية الدليل الإلكتروني في (الفرع الثاني) .

الفرع الأول: حجية الدليل الإلكتروني في ظل أنظمة الإثبات المختلفة:

نتناول هذه المسألة بحسب كل نظام من أنظمة الإثبات وذلك كما يأتي:

أولا: في ظل نظام الإثبات الحر(النظام اللاّتيني): تأخذ الدول اللاّتينية بنظام الإثبات الحر وهو لا يثير صعوبات بشأن حجية الدليل الرقمي، لأن القاضي الجنائي يملك الحرية في تقديره، ومن ثمة الأخذ به من عدمه، حيث لا يخضع في ذلك لرقابة المحكمة العليا، وإنما لرقابة موضوعية بخصوص مبررات الأخذ به، وأخذت بذلك العديد من التشريعات مثل: فرنسا وتركيا واليونان والبرازيل والنمسا وسويسرا[2]، في حين تشترط بعض الدول أن يكون الدليل الإلكتروني مقروءا بعد استخراجه من الحاسوب أو من خلال شاشته. إن أدلة الحاسوب هي تطبيق من تطبيقات الدليل العلمي بما يتصف به من موضوعية وحياد ومشروعية لإقناع القاضي الجنائي الذي يجب عليه قبل الاقتناع به أن يُميّز بين قيمته العلمية أولا عن طريق الاستعانة بالخبراء والمختصين، وثانيا الظروف والملابسات التي وجد فيه الدليل فيمكن أن يرفضه إذا رأى وجوده لا يتناسب منطقيا مع وقائع القضية[3].

ثانيا: في ظل نظام الإثبات المقيد: تعتمد حجية الدليل الإلكتروني في ظل هذا النظام على تحديد أدلة الإثبات من قبل المشرع، وليس تقديرها من قبل القاضي، فالدول التي تأخذ بهذا النظام مثل: بريطانيا وأمريكا تفرض قيودا على هذه الأدلة حتى يمكن الأخذ بها مثل: اعتماد مبدأ تعاضد

- نظام الاثبات المقيّد(القانوني): يقوم هذا النظام على فكرة تقييد الإثبات عن طريق تحديد أدلة الإثبات وحالات تقديمها وحجيتها، فهو يرتكز على مبدأين أساسين هما: مبدأ تحديد أدلة الإثبات، ومبدأ تحديد حجية أدلة الإثبات.

- نظام الإثبات المختلط: وهو نظام توفيقي أو وسط بين نظام الإثبات الحر والمقيد، حيث تتراوح أحكامه بين التقييد والإطلاق، راجع سامي جلال فقي حسين، الأدلة المتحصلة، المرجع السابق، ص ص69-93، راجع أيضا، كوثر أحمد خالند، المرجع السابق، ص31.

[1] بروتوكول*(TCP/IP)* اختصار لكلمة *(transmission control protocol/internet protocol)* وهما بروتوكولين معا وظيفتهما الاتصال بين عدة حواسيب عبر شبكة الإنترنت يعملان بشكل متزامن فمثلا بروتوكول*(IP)* الذي يشكل بروتوكول الإنترنت هو المسؤول عن تزامن حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها، وهو يتكون من أربعة أجزاء وكل جزء يتكون من أربعة خانات، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني إلى مزود الخدمة، والثالث لمجموعة الحسابات الآلية، والرابع يحدد الحاسوب الذي تم الاتصال به، راجع، خالد ممدوح إبراهيم، فن التحقيق، المرجع السابق، ص ص303-304، راجع أيضا، عبد الفتاح بيومي حجازي، الدليل الجنائي، المرجع السابق، ص ص63-64.

[2] هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، النسر الذهبي، القاهرة، مصر،2002، ص43 وما بعدها.

[3] سامي جلال فقي حسين، الأدلة المتحصلة، المرجع السابق، ص ص75-76.

الأدلة في التشريع البريطاني[1]. كما يحدد القانون الألماني على سبيل الحصر وسائل الإثبات التي يتعين على القاضي قبولها كسماع أو سؤال المتهم وشهادة الشهود وتقارير الخبراء[2]. في الشأن نفسه يستبعد المشرع الأمريكي الأدلة التي يمكن الحصول عليها بالمخالفة للحقوق الدستورية كالحجز والمصادرة والتفتيش غير المشروع[3]. إن دور القاضي في هذا النظام هو دور سلبي فإذا لم تكن هذه الشروط متوفرة، لا يستطيع الحكم بالإدانة بصرف النظر عن اعتقاده الشخصي حتى لو كان يميل إلى إدانة المتهم[4].

كما تبرز في ظل هذا النظام صعوبات في مجال إثبات الجرائم الإلكترونية، مما يستوجب إدخال تعديلات تتلاءم وطبيعة هذه الجرائم، نظرا للطفرة التكنولوجية الحاصلة في مجال المعلوماتية وشبكة الإنترنت، حيث لُوحظ بعض التغييرات على حدّة هذا النظام، بحيث صار يقبل بمبدإ حرية القاضي في تقدير الأدلة، فقاعدة حرية القاضي الجنائي في الاقتناع معترف بها تقريبا لدى جميع التشريعات القانونية مع اختلاف الصياغة في القوانين، ففي النظام اللاتيني تسمى بمبدإ الاقتناع القضائي، أما في النظام الأنجلوسكسوني فتسمى بالإدانة بدون أي شك معقول، أو الإدانة الخالية من أي شك[5].

ثالثا: في ظل نظام الإثبات المختلط: يعتبر نظام الإثبات المختلط نظام وسط، أي نظام توفيقي بين نظام الإثبات الحر ونظام الإثبات المقيد، حيث تتراوح أحكامه بين التقييد والإطلاق، كما جاء هذا النظام لتلافي الانتقادات الموجهة للنظامين السابقين، فيُجنب تعسف القاضي في نظام الإثبات الحر وخروجه عن جادة الصواب، كما يخفّف من الدور السلبي المحض للقاضي في النظام المقيد بأن يمنح له الحرية في تقدير ما يعرض عليه من أدلة[6]، كما قد يكون التوفيق بين النظامين عندما يحدد القانون أدلة معينة للإثبات في بعض الوقائع دون الأخرى، أو يطلب شروطا في بعض الحالات، أو

---

[1] يقصد بهذا المبدأ: تعزيز دليل بدليل آخر، فمثلا الشهادة لا تكفي وحدها في بعض الحالات، حيث يجب توافر دليل آخر معزّز لها كشهادة أخرى مستقلة عنها، أو دليل آخر كخبرة أو مستند، فإذا لم يتوافر هذا الدليل المساند حكم القاضي بالبراءة، راجع سامي جلال فقي حسين، الأدلة المتحصلة، المرجع نفسه، ص83.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص ص181-182.

[3] سامي جلال فقي حسين، الأدلة المتحصلة، المرجع السابق، ص ص81-83.

[4] هلالي عبد الإله أحمد، حجية المخرجات، المرجع السابق، ص50.

[5] سامي جلال فقي حسين، الأدلة المتحصلة، المرجع السابق، ص84.

[6] أُقترح النظام المختلط من طرف الأستاذ:(روبسيير) *(Robsir)* أمام الجمعية التأسيسية الفرنسية سنة1971، حيث كان هذا الاقتراح مكوّنا من جزئين: يتمثل الأول في عدم الحكم على المتهم إذا لم تتوفر ضده أدلة حددها القانون، والثاني عدم الحكم بإدانة المتهم حتى إذا توافرت أدلة قانونية، لكن هذه الأدلة لم تحقق قناعة القاضي. المرجع نفسه، ص93.

يعطي القاضي الحرية في تقدير الأدلة كالقانون الياباني الذي يحصر طرق الإثبات المقبولة في أقوال المتهم وشهادة الشهود والخبرة المنجزة من طرف الخبراء[1].

لكن بالمقابل أين موقف المشرع الجزائري من كل هذا؟ هذا ما سنعرفه في الفرع الموالي.

الفرع الثاني: موقف المشرع الجزائري:

لم تفرد تشريعات الدول المنتمية للنظام اللاتيني كفرنسا وغيرها من الدول المتأثرة بها ومنها الجزائر، نصوصا خاصة بقبول الدليل الإلكتروني، وهذا على أساس استنادها لمبدإ حرية الإثبات في المواد الجنائية تطبيقا لنظام الإثبات الحر، حيث تنص المادة (427) (ق.إ.ج.ف) على:" ما لم يرد نص مخالف يجوز إثبات الجرائم بجميع طرق الإثبات، ويحكم القاضي بناء على اقتناعه الشخصي..."[2]، تقابلها المادة (212) من (ق.إ.ج.ج) التي تنص على: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص، ولا يصوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه". من جهة أخرى يأتي إدراج المشرع لهذه المادة ضمن الأحكام المشتركة بطرق الإثبات، مما لا يدع للشك في تطبيقها أمام كل الجهات القضائية الجزائية، وبالتالي اعتمد المشرع الجزائري نظام الإثبات الحر كأصل ونظام الإثبات المقيد كاستثناء.

وعليهساير المشرع الجزائري الاتجاه العالمي السائر نحو الاعتراف أكثر فأكثر بحجية الأدلة الإلكترونية على اختلاف أنواعها، ولم يكتف بالنصوص التي تعتد بأدلة الإثبات الإلكتروني في المعاملات المدنية مثل: الإثبات بالكتابة في الشكل الإلكتروني[3] أو التوقيع والتصديق الإلكترونيين[4]، بل أقر جملة من الإجراءات الخاصة وهذا بموجب القانون رقم:09-04 المؤرخ في:05 غشت سنة2005 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

---

[1] هلالي عبد الإله أحمد، حجية المخرجات، المرجع السابق، ص59.

[2] ***Article 427 du (CPPF) :***

" Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et

Contradictoirement discutées devant lui".

[3] تنص المادة (323 مكرر1) من القانون رقم:05- 10 المؤرخ في:2005/06/20 المعدل والمتمم للقانون المدني على:" يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها.

[4] تنص المادة (1/02) من القانون رقم:15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين على: "يقصد بما يأتي: التوقيع الالكتروني: بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق".

والاتصال ومكافحتها[1]، حيث نص على مراقبة الاتصالات الإلكترونية وحفظ المعطيات المتعلقة بحركة السير وإلزام مؤدي الخدمات بحفظ وتسجيل معطيات زبائنهم، إضافة إلى كيفية تفتيش المنظومة المعلوماتية وحجز المعطيات وتجميع الأدلة الإلكترونية والاستعانة بكل شخص له مؤهلات لمساعدة الجهات القضائية المختصة- سنتطرق إلى هذه الإجراءات في (الفصل الثاني من الباب الثاني) - ومع ملاحظة أن هناك صعوبات فنية بخصوص استخدام *(TCP/IP)* في الإثبات الجنائي منها أن بروتوكول الإنترنت *(IP)* عبارة عن وحدة معلوماتية تحتوي على معلومات عن الكمبيوتر المعني وليس عن الأشخاص، فمن الصعوبة إثبات أن شخصا محددا قام بالفعل، لكن يبقى استخدامه كقرينة ضد ملك الجهاز إلى حين ثبوت العكس[2]، وأخيرا نستنتج أن هناك اعترافا صريحا من المشرع الجزائري بحجية الأدلة الإلكترونية في الإثبات الجنائي.

نتيجة لانتشار الجرائم الإلكترونية بكافة أنواعها، وقصد تحقيق الفعالية في مكافحتها، هناك اتجاه دولي للاعتراف بحجية المراسلات الإلكترونية بمختلف أنواعها والاعتراف بحجية الملفات المخزنة في النظم ومستخرجات الحاسوب والبيانات المسترجعة ، وحجية الملفات ذات المدلول التقني البحت، والإقرار بالإثبات بالكتابة في شكلها الإلكتروني وبصحة التوقيع الإلكتروني وتساويه في الحجية مع التوقيع الفيزيائي، والتخلي شيئا فشيئا عن أية قيود تحدّ من الإثبات في البيئة التقنية ومع كل هذا يجب مراعاة المبادئ والشروط التي تحكم الأدلة الإلكترونية، كمبدإ المشروعية، ومبدإ وجوب مناقشة الأدلة، ومبدإ اليقينية، وتأمين الدليل الرقمي ضد التلاعب، إضافة إلى صحة الوقائع الواردة بالدليل[3] .

المطلب الثالث: سلطة القاضي الجنائي في تقدير الدليل الإلكتروني

يعتبر مبدأ حرية الاقتناع الشخصي للقاضي الجزائي[4] من أهم عناصر الإثبات في الدعوى الجنائية، فالقاضي حر بأن يأخذ بالأدلة التي يراها مناسبة للكشف عن الحقيقة وله أن يتحرى بنفسه صدق الأدلة، كما أنه حر في تقدير جميع الأدلة بما فيها الأدلة الرقمية، وله الحق في أن يستمد

---

[1] المواد (12-04) من القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص108.

[3] صبرينة بن سعيد، الأطروحة السابقة، ص ص242-243.

[4] يتميز الاقتناع الشخصي للقاضي الجزائي بخاصيتين هما:

- الخاصية الأولى: تعبّر عن حالة ذهنية مبنية على الاحتمال وأن العبرة ليست بكثرة الأدلة، وإنما بما تتركه من أثر في نفسية القاضي الذي سيحدد مصير الدعوى الجزائية إما بالبراءة أو الإدانة.
- الخاصية الثانية: تتمثل في أن القاضي حر في أن يأخذ عقيدته أو اقتناعه من أي دليل يراه مناسبا لإظهار الحقيقة، نعيم سعيداني آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة الحاج لخضر باتنة، 2013، الجزائر، ص226.

اقتناعه وعقيدته من أي مصدر يطمئن إليه. كما أن الاقتناع في دلالته القانونية يعني: حالة إدراك يسلم معها العقل تسليما جازما بثبوت أو نفي واقعة أو عدة وقائع، استنادا لقواعد المنطق القائمة على الاستقراء والاستنتاج والمستمدة من أدلة وبراهين قضائية حاسمة، وحرية الاقتناع هي حرية خاصة بالقاضي، من خلالها يعمل سلطته التقديرية ويبسطها على الأدلة الجنائية. فبالرغم من أن النيابة العامة عليها أن تقيم الدليل على الإدانة والمتهم عليه أن ينفي هذا الدليل، إلا أن التزام القاضي الجنائي بإدراك الحقيقة الواقعية أو المادية استجابة لمقتضيات التجريم، جعلت له دورا إيجابيا يدرك بمقتضاه الحقيقة ويختلف عن دور القاضي المدني الذي يقتصر على الموازنة بين الأدلة التي يقدمها الأطراف دون البحث عن حجج أخرى من تلقاء نفسه.

سنتناول سلطة القاضي الجنائي في تقدير الدليل الإلكتروني في (الفرع الأول)، ثم نتطرق إلى الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الإلكتروني في (الفرع الثاني).

الفرع الأول: مبدأ الاقتناع القضائي:

إن السائد في الفقه هو أن سلطة القاضي الجنائي يحكمه مبدأ الاقتناع القضائي، وأن هذا المبدأ يؤدي إلى نتيجتين هما: الأولى حرية القاضي في قبول الأدلة والثانية حرية القاضي في تقدير الأدلة[1]، هذه الأخيرة تمثل مسألة قانونية لامجال لإعمال سلطة القاضي التقديرية، حيث أن المشرع حسم هذه المسألة بتحديده للنموذج القانوني للدليل الخاضع لتقدير القاضي، فمتى توافرت شروط الدليل طبقا لمبدإ الشرعية الإجرائية[2]، وجب على القاضي إخضاعه لعملية تقديره. كما أن القاضي

---

[1] زيدان فاضل، المرجع السابق، ص93.

[2] من الشروط الواجب توافرها في الأدلة لاقتناع القاضي بها نذكر:

أولا: ينبغي أن يستمد القاضي الجنائي اقتناعه من أدلة لها أصل في أوراق الدعوى سواء كانت في محاضر الاستدلال أو التحقيق أو المحاكمة، وسواء كانت هذه الأدلة قد قُدمت من قِبل أطراف الدعوى أو إن القاضي حثّهم على تقديمها أو إنه قد قام بدور إيجابي للبحث عن مثل هذه الأدلة التي تفيد الدعوى وتوصله إلى الحقيقة. كذلك ينبغي أن يكون اقتناع القاضي الجنائي قد بُني على دليل مستمد من إجراء بُوشر في حضور المتهم أو اطلع عليه هو أو محاميه، فضلا عن عدم جواز اعتماد القاضي على أدلة ووقائع استمدها القاضي من أوراق قضية أخرى لم تكن مطروحة على بساط البحث تحت نظر أطراف الدعوى.

ثانيا: ينبغي أن يستمد القاضي الجنائي اقتناعه من أدلة طرحت في الجلسة للمناقشة ويقوم هذا الشرط على مبدأ الشفوية والمواجهة في المحاكمة الجنائية، وهو مبدأ أساسي في الإجراءات الجنائية إذ ينبغي على القاضي أن يطرح كل دليل مقدم في الدعوى للمناقشة أمام الخصوم حتى يكونوا على بيّنة مما يقدم ضدهم من أدلة حتى يتمكنوا من مواجهة هذه الأدلة والرد عليها، ويترتب على ذلك أنه لا يجوز للقاضي الجنائي أن يبني اقتناعه على دليل قدمه أحد أطراف الدعوى، إلا إذا عُرض هذا الدليل في جلسة المحاكمة وخضع للمناقشة بحيث يعلم به سائر الأطراف. ومع ذلك فإن القاضي الجنائي في تكوين عقيدته حر في أن يعتقد أو لا يعتقد في قيمة الأدلة، والأخذ ببعضها الآخر، فهو حر في اقتناعه بالدليل الذي يراه طالما تحقق فيه شرط ثبوته بالأوراق وطرحه بالجلسة، كما أن طرح الدليل بالجلسة لا يحول دون حق القاضي في الأخذ بما ورد في التحقيقات الأولية طالما اقتنع بها.

يمارس سلطته التقديرية بخصوص تقدير قيمة الدليل لإثبات الحقيقة، وأنه تم استخلاصه بطريقة مشروعة[1].

يُخوّل مبدأ الاقتناع القضائي للقاضي الجزائي حرية واسعة في البحث عن الأدلة ومنها الأدلة الإلكترونية وتقديرها، فإن استراح إليها ضميره ووجدها كافية ومنطقية فيمكنه أن يستمد قناعته ويُعوّل عليها في الحكم الذي ينتهي إليه[2] غير أنها حرية محكومة بضوابط معينة، بما يضمن كشف الحقيقة.

فمع ظهور الدليل الرقمي للإثبات في الجرائم الإلكترونية، اضطر القاضي معه لكشف أنماط جديدة من الجرائم في مقابل نقص الثقافة المعلوماتية، ناهيك عن المشكلات التي تثيرها الطبيعة العلمية للدليل الرقمي، فهو دليل غير مرئي قابل للمحو والتعديل بما يثير صعوبة كبيرة في استخلاصه، مما يؤدي في الأخير إلى إنقاص قيمته ونسبية الاستناد عليه في إثبات الجرائم الإلكترونية[3].

في هذا الشأن، كرّس المشرع الجزائري هذا المبدأ بموجب المادتين(212) و(307) من (ق.إ.ج.ج)، حيث تنص المادة (307) على :"يتلو الرئيس قبل مغادرة المحكمة ...إن القانون لا يطلب من القضاة أن يقدموا حسابا على الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما..."، وهي مستوحاة من نص المادة (353) من (ق.إ.ج.ف)[4].

ثالثا: ينبغي أن يكون اقتناع القاضي الجنائي مبنيا على دليل مشروع، ومستمد من إجراءات صحيحة، ويُؤسّس هذا الشرط على قاعدة مشروعية الدليل الجنائي أو قاعدة الشرعية الإجرائية.، راجع، حسين بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص ص605-607 ، راجع أيضا، ضياء على أحمد نعمان، المقال السابق، ص ص309-315.

[1] نابر نبيل عمر، المرجع السابق، ص179.

[2] حسين بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص602.

[3] عائشة بن قارة مصطفي، المرجع السابق، ص239.

[4] ***Article 353 du (CPPF) :***

"Avant que la cour d'assises se retire, le président donne lecture de l'instruction suivante, qui est, en outre, affichée en gros caractères, dans le lieu le plus apparent de la chambre des délibérations :

" Sous réserve de l'exigence de motivation de la décision, la loi ne demande pas compte à chacun des juges et jurés composant la cour d'assises des moyens par lesquels ils se sont convaincus, elle ne leur prescrit pas de règles desquelles ils doivent faire particulièrement dépendre la plénitude et la suffisance d'une preuve ; elle leur prescrit de s'interroger eux-mêmes dans le silence et le recueillement et de chercher, dans la sincérité de leur conscience, quelle impression ont faite, sur leur raison, les preuves rapportées contre l'accusé, et les moyens de sa défense. La loi ne leur fait que cette seule question, qui renferme toute la mesure de leurs devoirs : " Avez-vous une intime conviction ? ".

الفرع الثاني: الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الإلكتروني:

إن القاضي الجنائي وإن تمتع بسلطة واسعة في تقديره للأدلة بما في ذلك الدليل الإلكتروني حيث ترك له المشرع سلطة واسعة، فله أن يتحرى الحقيقة بكافة الأدلة دون إلزامه بقيمة مسبقة لدليل ما حتى ولو كان دليلا علميا كالدليل الإلكتروني، أو تحديده لنوع معين من الأدلة لا يجوز الإثبات بغيرها، غير أن هذه السلطة وخلافا لما ذهب إليه الفقه، اعتبرها القضاء بأنها سلطة مطلقة وتحكميّة غير أن المشرع وضع لها ضوابط وهي بمثابة صمّام أمان إزاء انحراف القاضي عند ممارسته لها كي لا تختل الأحكام[1].

أولا: الضوابط المتعلقة بمصدر الاقتناع: في هذا الشأن يحكم اقتناع القاضي بالأدلة الإلكترونية ضابطان هما:

1- **شروط قبول الدليل الإلكتروني:** إن القاضي ليس حرا في تقدير أي دليل كان، بل هو حر فقط في تقدير الدليل الإلكتروني المقبول في الدعوى، بمعنى الحصول عليه بطريق مشروع إعمالا لمبدإ الشرعية الإجرائية، وبالتالي يستبعد في مقابل ذلك من المرافعة سائر الأدلة الإلكترونية غير المقبولة، لأنها لا تدخل ضمن عناصر تقديره[2]. وعليه لا يجوز للقاضي الاستناد إلى دليل استمد من إجراءات باطلة لأن ما بني على بال فهو باطل.

2- شرط وضعية الدليل الإلكتروني: من المعروف في القواعد الأساسية في الإجراءات الجنائية أنه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة ومقتضى ذلك أن يكون للدليل أصل ثابت في أوراق الدعوى وأن تتاح للخصوم فرصة الاطلاع عليه ومناقشته. ويقوم هذا الشرط على مبدإ الشفوية والمواجهة في المحاكمة الجنائية[3]، وهو مبدأ أساسي في الإجراءات الجنائية نص عليه المشرع الجزائري بموجب المادة (2/212) من (ق.إ.ج.ج) التي تنص على:"...ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه". إذ ينبغي على القاضي أن يطرح كل دليل مقدم في الدعوى للمناقشة أمام الخصوم في الجلسة حتى يكونوا على بيّنة مما يقدم ضدهم من أدلة قصد تمكينهم من مواجهتها ودحضها، ويترتب على ذلك أنه لا يجوز للقاضي الجنائي أن يبني اقتناعه على دليل قدمه

---

[1] زيدان فاضل، المرجع السابق، ص267.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص269.

[3] حسين بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص606.

أحد أطراف الدعوى، إلا إذا تم عرضه في جلسة المحاكمة وخضع للمناقشة بحيث يكون معلوما لكافة أطراف الدعوى[1].

ثانيا: الضوابط المتعلقة بالاقتناع ذاته: يتيح مبدأ الإثبات الجنائي حرية كبيرة للقاضي في تقدير عناصر الإثبات بما في ذلك الأدلة الرقمية، وعليه فإن تقدير كفاية أو عدم كفاية الدليل الإلكتروني في إثبات الجريمة الإلكترونية ونسبتها إلى مرتكبها أمر متروك لمحكمة الموضوع المعروض عليها الدليل، ولا تخضع في ذلك لرقابة محكمة النقض التي يقتصر دورها على مراقبة المنطق القضائي لمحكمة الموضوع عن طريق رقابتها على صحة تسبيب الحكم[2].

وعليه لبلوغ القاضي درجة الاقتناع التام للفصل في القضية، لابد له من شروط تتمثل أساسا في:

أ- **بلوغ الاقتناع القضائي درجة اليقين:** تقتضي العدالة أن يصدر القاضي حكمه عن اقتناع يقيني بصحة ما ينتهي إليه من وقائع لا مجرد الظن والاحتمال، لأن الشك يفسّر لصالح المتهم وذلك تطبيقا لقاعدة" الأصل في الانسان البراءة"، كما أن شرط اليقين هو شرط عام تستوي فيه الأدلة الرقمية مع الأدلة التقليدية. ويقوم اليقين القضائي على عنصرين: الأول شخصي يتمثل في ارتياح ضمير القاضي حول إدانة المتهم، والثاني موضوعي يقوم على أدلة من شأنها أن تؤدي لذلك وفقا لمقتضيات العقل والمنطق.

ب- **توافق الاقتناع القضائي مع مقتضيات العقل والمنطق:** ومعنى ذلك أن يكون استخلاص محكمة الموضوع لوقائع الدعوى استخلاصا معقولا سائغا. إن معيار معقولية الاقتناع بما في ذلك الأدلة الرقمية، هو أن تكون هذه الأدلة مؤدية إلى ما رتبه الحكم عليها من غير تعسف في الاستنتاج ولا تعارض مع مقتضيات العقل والمنطق[3].

المطلب الرابع: مدى تأثير مشكلات الدليل الإلكتروني على مبدأ اقتناع القاضي

رأينا سلفا أن المشرع الجزائري وافق الاتجاه العالمي السائر نحو الاعتراف أكثر فأكثر بحجية الأدلة الإلكترونية على اختلاف أنواعها، حيث يتمتع القاضي الجنائي بسلطة واسعة في تقديره للأدلة بما في ذلك الدليل الإلكتروني، فله أن يتحرّى الحقيقة بكافة الأدلة دون إلزامه بقيمة مسبقة لدليل ما حتى ولو كان دليلا رقميا. غير أن الدليل الرقمي يثير العديد من المشكلات نظرا لطبيعته التكوينية من جهة، وإجراءات الحصول عليه من جهة أخرى، فهو يتواجد في بيئة رقمية تعتمد نظاما ثنائيا مما

---

[1] عائشة بن قارة مصطفى، المرجع السابق، ص269، راجع أيضا، حسين بن سعيد الغافري، السياسة الجنائية، المرجع السابق ص606.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص276.

[3] المرجع نفسه، ص281.

قد يضعف من قيمته الإثباتية، وعليه سنتطرق إلى المشكلات الموضوعية التي تؤثر على مبدإ اقتناع القاضي في (الفرع الأول)، ثم للسبب نفسه نتناول المشكلات الإجرائية في (الفرع الثاني).

الفرع الأول: المشكلات الموضوعية للدليل الرقمي:

يثير الدليل الرقمي مشكلات موضوعية تتعلق أساسا بالخصائص المتفردة للدليل الرقمي، مما يشكل صعوبة بالغة لأجهزة البحث والتحري لاستخلاصه، قصد تقديمه للقاضي الجزائي الذي يعمل وفق مبدأ الاقتناع الشخصي، حيث يدفعه الأمر لبذل جهد إضافي لتقديره، مما قد يؤثر سلبا على اقتناعه، فيمكن تلخيص هذه المشكلات الموضوعية فيما يأتي:

أولا: الدليل الرقمي متنوع ومتطور: يشمل الدليل الرقمي كافة أشكال وأنواع البيانات الرقمية المتداولة، حيث يكون بينها وبين الجريمة رابط خاص، يتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني، وتعني هذه الخاصية أنه على الرغم من أن الدليل الرقمي في أساسه متحد التكوين بلغة الحوسبة، إلا أنه مع ذلك يتخذ أشكالا مختلفة، يمكن أن يظهر عليها كأن يكون بيانات غير مقروءة كما هو الشأن في حالة المراقبة عبر الشبكات والخوادم، وقد يكون بيانات مفهومة كما لو كان وثيقة معدة بنظام المعالجة الآلية، كما يمكن أن يكون صورة ثابتة أو متحركة كالأفلام الرقمية أو معدة بنظام التسجيل السمعي البصري، أو يكون مخزنا في البريد الإلكتروني*(e-mail)*، كما قد يكون مرتبطا بالتشفير، إذ يُعد هذا المفهوم تعبيرا عن اتساع قاعدة الدليل الرقمي، إذ يُمكن لهذه البيانات الرقمية سواء كانت منفردة أو مجتمعة أن تكون دليل براءة أو إدانة ضد المتهم[1].

فالأدلة الرقمية تتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات الحاسوب المادية *(Hardware)* إضافة إلى نظم وبرامج حاسوبية *(Software)*[2]. فالدليل الرقمي عبارة عن نبضات إلكترونية غير مرئية لا تفصح عن شخصية معينة، إذ يُمكن لمستعملي شبكة الإنترنت الاتصال دون الكشف عن شخصياتهم الحقيقية فضلا عن ذلك غالبا ما يكون الدليل الرقمي مرمزا أو مشفرا، كما يمكن تعديله أو محوه أو التلاعب فيه مما يقطع الصلة بين المجرم وجريمته[3]، وهنا تكمن صعوبة البحث والتحري عن الجرائم الإلكترونية لاستخلاص الدليل الرقمي الذي يحتاج لأفراد متخصصين في مجال تقنية المعلومات وعلى مستوى عال من التدريب، فضلا عن صعوبة اقتناع القاضي الجزائي به.

---

[1] نعيم سعيداني، المذكرة السابقة، ص124، راجع أيضا، صبرينة بن سعيد، الأطروحة السابقة، ص254.

[2] عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق، ص14.

[3] يوسف صغير، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو الجزائر، 2013، ص125، راجع أيضا، عائشة بن قارة مصطفي، المرجع السابق، ص252.

وأما بخصوص كون الدليل الرقمي دليلا متطورا، فهي خاصية تتماشى والتطورات التقنية المذهلة في مجال صناعة الحوسبة والاتصال، إذ يرتبط الدليل الرقمي بالطبيعة التي تتمتع بها حركة الاتصال عبر شبكة الإنترنت والعالم الافتراضي اللّذين لا حدود لهما[1].

ثانيا: مشكلة الأصالة في الدليل الرقمي: إن الأصالة في الدليل الرقمي لها طابع افتراضي لا يرقى إلى مستوى الأصالة في الدليل المادي التقليدي، فهذه الأخيرة تعبر عن وضعية مادية ملموسة كما هو الشأن في الدليل الورقي أو البصمة الوراثية...إلخ، في حين أن الدليل الرقمي عبارة عن تعداد غير محدود من الأرقام الثنائية *(Binary Digits)*[2]. إن البيانات الموجودة داخل الحاسوب سواء كانت في شكل نصوص أو أرقام أو حروف أو صور أو فيديوهات، تتحول إلى صيغة رقمية، حيث ترتكز التكنولوجية الرقمية الحديثة على الرقمنة التي تعني ترجمة أو تحويل أي مستند إلى نظام ثنائي في تمثيل الأعداد يفهمه الحاسوب قوامه الرقمين الصفر والواحد (1−0)، وعليه فالكتابة في العالم الافتراضي ليس لها وجود مادي وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد وهو النظام الثنائي الرقمي وهو عبارة عن نبضات إلكترونية متواصلة الإيقاع، تستمد فاعليتها وحيويتها من الطاقة[3].

ونظرا لأهمية موضوع الأصالة في الدليل الرقمي، اعتمد المشرع منطق افتراض أصالة الدليل الرقمي، ومنها التشريع الأمريكي بنص القاعدة رقم:1001 البند (3)، حيث سمح استثناء بقبول الدليل الرقمي باعتباره مستندا أصليا مادام أن البيانات صادرة من كمبيوتر أو جهاز مماثل، وسواء كانت هذه البيانات مطبوعة أو مسجلة على دعامات وتعبر عن البيانات الأصلية بشكل دقيق، ومنه تتساوى الكتابة المادية من حيث الأصالة مع مخرجات الحاسوب بالرغم من أنها عبارة عن مجرد نسخ للبيانات الأصلية التي يحتويها الحاسوب أو في شبكة الإنترنت[4].

ثالثا: الدليل الرقمي من طبيعة تقنية: ينبئ الدليل الرقمي عن واقعة علمية شديدة التعقيد، إذ لا يمكن استخلاصه إلا باستعمال الأساليب العلمية والتقنية. وعليه تتطلب الطبيعة التقنية للدليل الرقمي أن يكون هناك توافق بين الدليل المتحصل عليه والبيئة التي جاء منها، فمثلا لا ينتج عن البيئة الافتراضية سلاح الجريمة أو بصمات المجرم، وإنما ما ينتج عن تقنية المعلومات هو نبضات

---

1 نعيم سعيداني، المذكرة السابقة، ص124.

2 عائشة بن قارة مصطفى، المرجع السابق، ص252.

3 نعيم سعيداني، المذكرة السابقة، ص126.

4 عائشة بن قارة مصطفي، المرجع السابق، ص253.

إلكترونية غير مرئية، مما يجعلنا نستنتج أنه ليس هناك دليل الكتروني خارج بيئته الرقمية، فلكي يكون هناك دليل رقمي يجب أن يكون مستوحى أو مستنبطا من البيئة الرقمية الموجود فيها[1].

ونظرا للطبيعة التقنية للدليل الرقمي يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها القيمة العلمية نفسها والحجية الثبوتية، الشيء الذي لا يتوافر في أنواع الأدلة الأخرى التقليدية، مما يشكل ضمانة أكيدة للحفاظ على الأدلة الرقمية ضد الفقد أو المحو أو التعديل[2]، ونظرا لما تتطلبه العملية من جانب تقني معقد، أجاز المشرع الجزائري نسخ و إفراغ المعطيات على دعامة تخزين إلكترونية تكون قابلة للحجز مثل: الأقراص المرنة والأقراص المضغوطة أو المدمجة والذاكرة الومضية...إلخ. وهذا بموجب نص المادة (06) من القانون 09-04 :"عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهما على دعامة تخزين إلكترونية تكون قابلة للوضع والحجز في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية..." .

رابعا: صعوبة فهم الدليل المتحصل من الوسائل الإلكترونية:لا شك في أن طبيعة الدليل تنعكس عليه، فالدليل الرقمي قد يكون مضمونه مسائل فنيّة لا يقوى على فهمها إلا الخبير المتخصص، فهو يستخلص من عمليات فنية معقدة عن طريق التلاعب في نبضات وذبذبات إلكترونية وعمليات أخرى غير مرئية قد تصل إلى غاية التخيليّة في شكلها وحجمها ومكانها غير المعلن[3]، فإن الوصول إليه وفهم مضمونه قد يكون في غاية الصعوبة.

تثير الطبيعة غير المادية للبيانات المخزنة بالحاسب الآلي والطبيعة المعنوية لوسائل نقل هذه البيانات مشكلات عديدة في الإثبات الجنائي، وبالنظر إلى أن طبيعة هذه العمليات يصعب أن تخلف وراءها آثارا مادية ملموسة تكشف عنها، فإن ذلك سيزيد من صعوبة عمل المحققين، خاصة إذا كان الحاسوب متصلا بشبكة الإنترنت فقد يستعصى عليهم فهم الأدلة المتحصلة عن هذه الوسائل بسبب تعقيدها، لذا فالأمر يحتاج إلى خبرة فنية ومقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجوده واختيار أفضل السبل لاستخلاص الدليل الرقمي.

من جهة أخرى، فإن فهم الأدلة الفنية التي تتحصل من الوسائل الإلكترونية يتطلب أيضا تدريب جهات الضبط القضائي والتحقيق والقضاء –القاضي الجنائي–على فهم طبيعة المعطيات التي تقع

---

[1] صبرينة بن سعيد، الأطروحة السابقة، ص254.

[2] عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق، ص15.

[3] المرجع نفسه، ص14.

عليها الجرائم الإلكترونية، والعمل على إلمامهم بمكونات الحاسوب وكيفية عمله ومعرفة اللّغة التي تتعامل بها، تمهيدا لاستخلاص دليل رقمي له حجية يؤثر إيجابا في اقتناع القاضي به.

الفرع الثاني: المشكلات الإجرائية للدليل الرقمي:

لا تقف صعوبة إثبات الجرائم الإلكترونية عند تعذر الوصول إلى الأدلة التي تكفي لإثباتها وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة، وسنتطرق هنا إلى حالتين هما: ارتفاع تكاليف الحصول على الأدلة الرقمية، ونقص الخبرة الفنية والتقنية لدي سلطات الاستدلال والتحقيق والقضاء في مجال تقنية المعلومات.

أولا: ارتفاع تكاليف الحصول على الأدلة الرقمية: غالبا ما يتم اللّجوء إلى الخبرة الرقمية للتعامل مع إثبات الجرائم الإلكترونية، إلا أن إنجاز هذه الخبرة يشكل عبءا ثقيلا على كاهل العدالة الجنائية، لما يتطلبه ذلك من مصاريف كبيرة للحصول على الدليل الرقمي، ويرجع ذلك إلى الطبيعة الخاصة لهذا النوع من الأدلة الذي يختلف حتما عن الأدلة التقليدية المعروفة سواء من حيث طبيعتها أو تكاليف الحصول عليها. ويبرز الأمر في ظل غياب منظمات متخصصة كالجامعات والمعاهد حيث يتطلب الأمر اللّجوء إلى الخبرة الأجنبية ممثلة في شركات متخصصة، مما يجعل التكاليف تخضع للسعر العالمي المقرر في اللوائح المالية لتلك الشركات.[(1)]

وبقصد تخفيض هذه التكاليف يجب على كل دولة إنشاء وحدات تابعة لأجهزة البحث والتحري متخصصة ومؤهلة وعلى مستوى عال من التدريب على استعمال وسائل تقنية المعلومات لخلق توازن بين وسائل ارتكاب الجرائم الإلكترونية ووسائل الكشف عنها في ظل بيئة افتراضية تتسم بتحديات كبيرة، وهذا ما قام به المشرع الجزائري بهدف تحقيق الفعالية وتخفيض التكاليف. حيث أنشأت المديرية العامة للأمن الوطني بالمخبر المركزي للشرطة العلمية بالجزائر العاصمة خلية للإعلام الآلي مهمتها البحث والتحري عن الجرائم الإلكترونية، كما تم تدعيم مراكز الأمن الولائي بفرق متخصصة بالتحقيق في هذا المجال تعمل بالتنسيق مع المخبر المركزي، وهو الأمر نفسه بالنسبة للقيادة العامة للدرك الوطني.

ثانيا: نقص المعرفة التقنية لدى جهات البحث والتحري: انعكست الطبيعة الخاصة للدليل الرقمي على عمل الجهات المكلفة بالبحث والتحري، حيث يتطلب الكشف عن الجريمة الإلكترونية وإثباتها اكتساب أفراد هذه الأجهزة مهارات خاصة تمكنهم من مواكبة التطورات الحاصلة في مجال

---

[1] أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت، المرجع السابق، ص291، راجع أيضا، عائشة مصطفى بن قارة المرجع السابق، ص255.

تقنية المعلومات، إذ أن البيئة الإلكترونية تسمح للمجرم ارتكاب جريمته بضغطة زر، فهي تسمح أيضا لجهة البحث والتحري إمكانية كشفه وملاحقته وتوقيع العقاب عليه، بشرط تحكم هؤلاء في التقنية المعلوماتية خاصة وأنها تتطور بشكل سريع جدا.

وإذا كان لندب الخبراء أهمية في الجرائم التقليدية، فإن أهميتها أكثر وضرورتها أشد في إجراءات جمع أدلة المكونات المعنوّية في كل وحدات التخزين وتحليلها وكشف أي تلاعب في البرامج والمعلومات، غير أن ذلك لا يعني عدم الاكتراث بمسألة تأهيل سلطات البحث والتحري وتزويد أفرادها بالمعرفة العلمية والتقنية والتدريب اللاّزمين لكشف وإثبات الجرائم الإلكترونية. لذلك نجد الكثير من الدول المتقدمة قد اهتمت بتدريب المحققين في الجرائم الإلكترونية، كما دعا المجلس الأوروبي في إحدى توصياته سنة 1999 إلى ضرورة تدريب الشرطة وأجهزة العدالة بما يواكب التطور المتلاحق لتقنية المعلومات واستخدامها لتحقيق التوازن بين وسائل ارتكاب الجريمة وبين سبل مواجهتها، وعقدت كذلك المنظمة الدولية للشرطة الدولية العديد من الدورات التدريبية لمحققي جرائم الحاسب الآلي[1].

وفي الأخير تجدر الاشارة –كما رأينا سلفا–إلى أنه من بين الشروط الخاصة لممارسة القاضي حريته في الاقتناع، أن تكون عقيدته واقتناعه قد أستمدا من أدلة طُرحت ونُوقشت بالجلسة، وأن يكون اقتناعه مبنيا على دليل مستمد من إجراء صحيح، ومبنيا على أدلة مستساغة عقلا وعلى اليقين الذي ينفي الأصل وهو البراءة، وأن لا يؤسّسه على قرينة واحدة، وهذا برغم ما يطرحه الدليل الرقمي من مشكلات موضوعية وإجرائية قد تؤثر على مبدإ اقتناع القاضي الجزائي، لذا يجب أيضا على السلطات القضائية تخصيص دورات تكوينية لفائدة القضاة في مجال مكافحة الجرائم الإلكترونية خاصة ما تعلق بفهم الأدلة الإلكترونية وطرق استخلاصها.

---

[1] مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، المرجع السابق، ص48، راجع أيضا، يوسف صغير، المذكرة السابقة، ص131.

خلاصة الفصل الأول:

تعرفنا في هذا الفصل على مجموعة من الإجراءات التقليدية التي نص عليها المشرع الجزائري بخصوص استخلاص الدليل عموما، وحاولنا اسقاطها على عملية جمع الدليل الرقمي في مجال الجرائم الإلكترونية كإجراء المعاينة في مسرح الجريمة الإلكتروني والخبرة الرقمية ودور الشاهد المعلوماتي والتزاماته ومدى انطباق حالات التلبس على الجريمة الالكترونية. والتي خلصنا فيها إلى عدم كفاية هذه الإجراءات التقليدية في استخلاص الدليل الرقمي، بما يحتم على المشرع إعادة صياغة هذه النصوص أو استحداث أخرى جديدة لمواكبة التطورات التقنية المتلاحقة في مجال مكافحة الجريمة الإلكترونية.

وعليه سارع المشرع إلى تحديث سياسته الجنائية الإجرائية بتعديل قانون الإجراءات الجزائية بهدف جعله يتطابق مع ما جاء في المواثيق والاتفاقيات الدولية في هذا المجال، وذلك بإدراج قواعد إجرائية جديدة تتمثل في أساليب بحث وتحري خاصة تتلائم وطبيعة هذه الجرائم لاستخلاص الدليل الإلكتروني الذي تختلف طبيعته عن الدليل التقليدي، وهذا بموجب المواد (65 مكرر5 – 65 مكرر18) من (ق.إ.ج.ج)، كاعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرّب، وفي الوقت نفسه أحاطها بجملة من الضمانات بهدف عدم المساس بحرمة الحياة الخاصة للأفراد المكفولة دستوريا، رغم تسجيل بعض الإشكالات القانونية والعماية أثناء تطبيقها.

في السياق نفسه، وبهدف تسهيل عمل الأجهزة القضائية المكلفة بالتحريات والتحقيقات في إطار مكافحة هذا النوع المستحدث من الجرائم ومنها الجرائم الإلكترونية، سارع المشرع إلى تمديد الاختصاص القضائي لبعض المحاكم بموجب المرسوم التنفيذي رقم:06-348 المؤرخ في:2006/10/05 ووكلاء الجمهورية بموجب المادة(2/37) وقضاة التحقيق بموجب المادة(2/40) كما قام أيضا بتمديد الاختصاصات المكانية للضبطية القضائية بموجب المادة(7/16). من جهة أخرى، وسّع المشرع من الاختصاص المحلي للنيابة العامة في مجال تتبع الجرائم الإلكترونية وأجبرها بأن تباشر إجراءات المتابعة الجزائية تلقائيا، وذلك في المواد(144 مكرر –144 مكرر2) من (ق.ع.ج) والمتعلقة بجرائم القذف باستعمال أي وسيلة إلكترونية أو معلوماتية. كما لم يقتصر المشرع على تمديد الاختصاص القضائي في مفهومه التقليدي المادي فقط، بل تجاوز ذلك إلى تمديد الاختصاص في العالم الافتراضي، وذلك حينما يتعلق الأمر بتفتيش المنظومة المعلوماتية عن بعد بموجب نص المادة (5) من القانون رقم: 09-04.

وأخيرا تطرقنا إلى ماهية الدليل الإلكتروني ومدى قبوله من طرف الأنظمة القضائية وحجيته في الإثبات الجنائي، حيث برز بقوة اتجاه دولي للاعتراف بحجية المراسلات الإلكترونية بمختلف أنواعها والاعتراف بحجية الملفات المخزنة في النظم ومستخرجات الحاسوب والبيانات المسترجعة. كما تطرقنا

إلى سلطة القاضي الجنائي في تقدير الأدلة الإلكترونية والضوابط التي تحكمه في ذلك، ومدي تأثير المشكلات الموضوعية والإجرائية للدليل الإلكتروني على مبدإ اقتناعه. وخلصنا في الأخير إلى إقرار التشريعات المقارنة بمبدأ الإثبات بالكتابة في شكلها الإلكتروني وبصحة التوقيع الإلكتروني وتساويه في الحجية مع التوقيع الفيزيائي، والتخلي شيئا فشيئا عن أية قيود تحد من الإثبات في البيئة الرقمية وهذا ما سايره المشرع الجزائري مجسدا ذلك في جملة من النصوص مثل: الإثبات بالكتابة في الشكل الإلكتروني بخصوص المعاملات المدنية(المادة 323 مكرر1) من (ق.م.ج) والتوقيع والتصديق الإلكترونيين(المادة 1/02 من القانون رقم:15-04 المؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين).

الفصل الثاني: القواعد الخاصة للوقاية من الجرائم الإلكترونية

تطرقنا في الفصل السابق إلى بعض الإجراءات التقليدية المتعلقة بجمع الدليل الإلكتروني وخلصنا إلى عدم كفايتها لاستيعاب كافة أشكال هذا النوع المستحدث من الجرائم، مما دفع بالمشرع الجزائري إلى استحداث أساليب بحث وتحرّي جديدة تتلائم وخطورة هذه الجرائم ضمانا لعدم إفلات المجرم من العقاب. ونظرا للطبيعة الخاصة للجرائم الإلكترونية، لم يكتف المشرع باستخدام هذه الأساليب حينما تقع الجريمة، ولكن أيضا قبل وقوعها، وهذا ما ترجمته سياسته الجنائية الإجرائية حينما وضع قواعد إجرائية خاصة هدفها الوقائية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك حماية للنظام العام ومقتضيات التحريات والتحقيقات القضائية الجارية.

وعليه صدر القانون رقم: 09-04 المؤرخ في 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي جاء لتكريس إطار قانوني أكثر ملائمة وانسجاما مع خصوصية وخطورة الجريمة الإلكترونية، كما أنه يجمع بين القواعد الإجرائية لقانون الإجراءات الجزائية من جهة، والقواعد الوقائية التي تسمح بالرصد المبكّر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها في عالم افتراضي لا حدود له في الزمان والمكان. كما أخذا المشرع بعين الاعتبار الاتفاقيات الدولية ذات الصلة بالموضوع وكذا التجانس مع النصوص الوطنية التشريعية التي سنّها إلى حد الآن مثل: تلك المتعلقة بمكافحة الفساد وتبييض الأموال وتمويل الإرهاب والمخدرات والمؤثرات العقلية. نص هذا القانون على جملة من الإجراءات الهامة خاصة ما تعلق بحالات اللّجوء إلى المراقبة الإلكترونية وتفتيش المنظومة المعلوماتية وحجز المعطيات والتزامات مقدمي الخدمات ومزودي خدمة الإنترنت والتعاون والمساعدة القضائية الدولية، والاستعانة بكل شخص له دراية وخبرة لمساعدة جهات التحقيق في الكشف عن الجرائم الإلكترونية...إلخ.

وعليه سنقسم هذا الفصل إلى ثلاثة مباحث، نتناول مراقبة الاتصالات الإلكترونية ومساعدة السلطات القضائية في (المبحث الأول)، ثم نتطرق إلى تفتيش المنظومة المعلوماتية وحجز المعطيات في (المبحث الثاني)، لنختم في الأخير بالحديث عن مجال التعاون والمساعدة القضائية الدولية بخصوص الجرائم الإلكترونية باعتبارها جرائم عابرة للحدود في (المبحث الثالث).

المبحث الأول: في مجال مراقبة الاتصالات الإلكترونية ومساعدة السلطات

مما لاشك فيه أن إجراء المراقبة الإلكترونية إضافة إلى تنفيذ الالتزامات الواقعة على عاتق مزودي الخدمات ومقدمي خدمة الإنترنت، وهو ما يؤدي في الأخير إلى حفظ المعطيات وتسجيل محتواها في حينها، هو مساس بالحق في الخصوصية الذي يُعد حقا أساسيا من حقوق الإنسان، وهو أمر ضروري لتحقيق العديد من حقوق الإنسان الأخرى، ويعتبر عنصرا أساسيا لمجتمع ديمقراطي حيث تنص المادة (12) من الإعلان العالمي لحقوق الإنسان على:" لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات"، وفي الشأن نفسه، نصت المادة (17) من العهد الدولي الخاص بالحقوق المدنية والسياسية على أنه "لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته. من حق أي شخص أن يحميه القانون من مثل هذا التدخل أو المساس"[1].

سنتطرق إلى مراقبة الاتصالات الإلكترونية وحالات اللّجوء إليها في (المطلب الأول)، ثم نتناول شروط مراقبة الاتصالات الإلكترونية وكيفية القيام بها في (المطلب الثاني)، لنتطرق بعدها إلى التزامات مقدمي الخدمات في (المطلب الثالث)، وأخيرا نتناول الالتزامات الخاصة بمقدمي خدمة الإنترنت في (المطلب الرابع).

المطلب الأول: مراقبة الاتصالات الإلكترونية وحالات اللجوء اليها

من طبيعة الجريمة الإلكترونية أنها تتم في وسط افتراضي يسمح للمجرم المعلوماتي بمحو آثار جريمته بضغطة زر وفي جزء من الثانية، مما يخلق صعوبات بالغة لسلطات البحث والتحري في الكشف عنها، خاصة إذا أرادت التحكم فيها بوسائل الرقابة التقليدية. لذا عمل المشرع الجزائري وعلى غرار باقي المشرعين على تكريس إطار قانوني ينسجم مع خطورة وخصوصية هذه الجريمة المستحدثة، وذلك باستحداث نصوص تتضمن القواعد الوقائية التي تسمح بالكشف المبكر للاعتداءات المحتملة والتعرف على مرتكبيها، فأجاز بذلك إجراء مراقبة الاتصالات الإلكترونية.

من جانب آخر، يعتبر تكريس المشرع لهذا الإجراء خطوة جريئة منه على اعتبار أنه يُعد من أخطر الإجراءات في إطار النظام الإجرائي عبر العالم الافتراضي، بسبب أنه يمُس مباشرة بالحق في

---

[1] العهد الدولي الخاص بالحقوق المدنية والسياسية: أُعتمد وعُرض للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم:2200(د-21) المؤرخ في: 16 ديسمبر 1966 ودخل حيّز النفاذ بتاريخ: 23 مارس 1976وفقا لأحكام المادة (49) منه، حيث يلزم الأطراف احترام الحقوق المدنية والسياسية للأفراد بما في ذلك الحق في الحياة وحرية الدين وحرية التعبير وحرية التجمع والحقوق الانتخابية وحقوق إجراءات التقاضي السليمة والمحاكمة العادلة...إلخ.

الخصوصية والحقوق المتفرعة عنها، بل وتعدى الأمر إلى استعمال الدول هذا الإجراء للتجسّس على رؤساء بعضها البعض مثل: فضيحة تجسّس وكالة الأمن القومي الأمريكية على هاتف كل من المستشارة الألمانية (انجيلا ميركل) والرئيس الفرنسي (فرانسوا هولاند)، ورئيسة البرازيل (ديلما روسوفو)، حيث تسببت هذه العملية في أزمة ديبلوماسية مع هذه الدول[1]. فما المقصود بالمراقبة الإلكترونية؟ ، وما هي حالات اللّجوء إليها؟. سنتناول المقصود بمراقبة الاتصالات الإلكترونية في (الفرع الأول)، ثم نتطرق إلى حالات اللّجوء إليها في (الفرع الثاني).

الفرع الأول: المقصود بمراقبة الاتصالات الإلكترونية:

يعتبر الحق في الخصوصية ليس مطلقا، وأي قيود عليه يجب ألا تكون بشكل تعسفي، وبالتالي فإن تلك القيود يجب أن تكون مدرجة بوضوح في القانون ولا تشكل بأي حال مجالا لانتهاكه. ومن جهة أخرى هو مقيد بالمصلحة العامة للمجتمع المتمثلة في مكافحة الجريمة بكافة أشكالها للحيلولة دون انتشارها، وعليه يوجد توازن بين مصلحة الفرد في الخصوصية وحق المجتمع في التصدي للجريمة والوقاية منها. في هذا الشأن لم يتطرق المشرع الجزائري شأنه شأن أغلب التشريعات المقارنة إلى تعريف مراقبة الاتصالات الإلكترونية، لكنه بالمقابل أوضح لنا مفهوم الاتصالات الإلكترونية بموجب المادة (02/و) من القانون رقم:09 - 04 المؤرّخ في: 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي تنص على:" يقصد في مفهوم هذا القانون ما يأتي...:

-الاتصالات الإلكترونية: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية. فالمشرع وسّع من مفهوم الاتصالات الإلكترونية ليشمل كل وسائل نقل المعلومات التي تتم بطريقة إلكترونية، كما عرّف لنا أيضا الاتصالات الإلكترونية بموجب نص المادة (05) من المرسوم الرئاسي رقم:15-261 المؤرخ

---

[1] أعلنت ألمانيا استنكارها الشديد إزاء قيام وكالة الأمن القومي الأميركي إلى غاية 2013 بالتجسّس على الهاتف النقّال للمستشارة الألمانية (أنجيلا ميركل) باستعمال برامج التجسّس عبر الإنترنت والاتصالات الهاتفية. من جانب آخر، نشر موقع ويكيليكس (*wikileaks*)، تقارير تشير إلى تجسّس واشنطن على ثلاثة رؤساء فرنسيين، مما دعا الرئيس الفرنسي (فرانسوا هولاند) إلى الدعوة لاجتماع عاجل لمجلس الدفاع الفرنسي لاتخاذ الخطوات المناسبة اتجاه أمريكا. وفي نفس الشأن ألغت رئيسة البرازيل نهاية 2013 زيارة للولايات المتحدة الأمريكية، إثر كشف الصحف عن تجسّس المخابرات الأمريكية على مكالماتها الشخصية إضافة إلى مكالمات ملايين البرازيليين، حيث طلبت البرازيل تفسيرات من الولايات المتحدة الأمريكية، واشترطت وقف هذه الأنشطة قبل إتمام الزيارة. أكثر تفاصيل حول الموضوع، راجع الموقع الرسمي لشبكة الأخبار العالمية رويترز *(REUTERS)* على الرابط الآتي: *http://ara.reuters.com/article/worldNews/idARAKCN0T014E20151111*،تاريخ الاطلاع:2016/10/01 على الساعة:15:48.

في:10/08/ 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي تنص على:" يقصد في مفهوم هذا المرسوم ما يأتي:

– الاتصالات الإلكترونية: كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية، بما في ذلك وسائل الهاتف الثابت والنقال..." وبذلك وسّع المشرع الجزائري مرة أخرى من مفهوم الاتصالات الإلكترونية والتي تتم بأي وسيلة إلكترونية حديثة كجهاز الفاكس والهاتف الثابت والنقال والبريد الالكتروني*(E-MAIL)* والاتصالات التي تتم عبر شبكة الإنترنت باستعمال برامج كثيرة مثل: برنامج *(Skype)* *(Messenger)*...إلخ.

في هذا الشأن ميّزت (إ.أ.م.إ.م) بين نوعين من المعطيات المعلوماتية محل الاعتراض: المعطيات المتعلقة بالتجميع في الوقت الفعلي لمعطيات المرور، والمعطيات المتعلقة بمحتوى الاتصال. فبالنسبة للمعطيات المتعلقة بالتجميع في القوت الفعلي لمعطيات المرور عرفتها (4/01) من الاتفاقية على أنها: "كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي والتي يتم إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا من سلسلة الاتصال، مع تعيين المعلومات التالية: أصل الاتصال، مقصد الاتصال، خط السير، ساعة وتاريخ الاتصال، حجم وفترة الاتصال أو نوع الخدمة"[1]، أما بالنسبة للمعطيات المتعلقة بالمحتوى فلم تعرفها الاتفاقية لكنها تشير إلى مضمون الاتصال أو محتوى الرسالة أو المعلومات المنقولة عن طريق الاتصال وفق نص المادة (21) من (إ.أ.م.إ.م).

وعليه أدرجت (إ.أ.م.إ.م) كل إجراء على حدة، فنصت بموجب المادة (20) على التجميع في الوقت الفعلي لمعطيات المرور، بما في ذلك مزودي الخدمات وذلك باستعمال الوسائل التقنية المتاحة على إقليم الدولة...إلخ[2]، أما اعتراض معطيات المحتوى فنصت عليه بموجب المادة (21)[1]. كما

---

[1] ***Article 1 – Définitions***

"Aux fins de la présente Convention, l'expression :...

d. «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent." convention européenne de la cybercriminalité, Op.Cit,p.3.

[2] ***Article 20 – Collecte en temps réel des données relatives au trafic***

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à

i. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1(a), elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15, convention européenne de la cybercriminalité, Op.Cit,p.11.

[1] **Article 21 – Interception de données relatives au contenu**

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes relativement à un éventail d'infractions graves à définir en droit interne, à :

a. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire ; et

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

ii. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1(a), elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des== ==données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

نصت المادة (29) من (إ.ع.م.ج.ت.م) على اعتراض معطيات المحتوى تحت عنوان: "اعتراض معلومات المحتوى"، حيث تنص على:

"1- تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يختص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من:

أ- الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة الطرف أو،

ب- التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

2- إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة(1-أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري لمعلومات المحتوى المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3- تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود خدمة بالاحتفاظ بسرية أي معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة".

فهذه المادة تلزم الدول الأعضاء باتخاذ الاجراءات الضرورية لجمع وتسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية على إقليمها والتي تبث بواسطة تقنية المعلومات.

وعلى النهج نفسه سار المشرع الجزائري حينما ميّز في القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الإتصال ومكافحتها، بين المعطيات المتعلقة بالمحتوى، وبين المعطيات المتعلقة بالمرور مع وجهة نظر مزدوجة للشروط القانونية الواجب توافرها من أجل الإذن بكل اجراء[1]. حيث نص على تجميع المعطيات المتعلقة بالمحتوى بموجب المادة (04) من القانون09-04 تحت عنوان "مراقبة الاتصالات الإلكترونية" ونص على تجميع المعطيات في الوقت الفعلي لمعطيات المرور بموجب المادة (11) من القانون نفسه تحت عنوان: "حفظ المعطيات المتعلقة بحركة السير".

بالرجوع إلى المفهوم الفقهي لمراقبة الاتصالات الإلكترونية الذي يعني:" العمل الذي يقوم به المراقب باستخدام الاتصالات الإلكترونية لجمع معطيات عن المشتبه فيه سواء أكان الخاضع للمراقبة شخصا أو مكانا، أو شيئا ومثال ذلك مراقبة أحد الأشخاص ممن قام باختراق الحاسب الآلي الخاص

---

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et15, convention européenne de la cybercriminalité, Op.Cit,pp.11-12.

[1] رشيدة بوكر، المرجع السابق، ص368.

بالمجني عليه أو القيام بإعداد بريد إلكتروني مستنسخ في مراقبة المشتبه فيه عند إرساله أو استقبال لصور دعارة للأطفال عبر الإنترنت، وإفراغ ما تسفر عنه المراقبة الإلكترونية في تقارير أمنية" [1]. أو هي:" مراقبة شبكة الاتصالات"[2].

حيث ظهرت تقنية المراقبة الإلكترونية في إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفيدرالي الأمريكي *(FBI)* باستعمال أسلوب يدعى*(DCS1000)*، وتقوم فكرته على تتبع الرسائل الإلكترونية عبر أية شبكة معلومات توفر خدمة الإنترنت، حيث يقوم المكتب الفدرالي بإذاعة تلك الرسائل. من جانب آخر اعترضت على ذلك المجموعات المدافعة عن الخصوصية واعتبرته مقدمة للمساس بجملة الحقوق المحمية دستوريا كسرية المراسلات...إلخ. ولكن بالمقابل، اعتبر مكتب التحقيقات الفيدرالي أنه يقوم فقط بمراقبة الرسائل التي لها علاقة بالجرائم الجنائية[3].

يتضح لنا من المفاهيم السابقة أن هذا الإجراء في طبيعته يمس بحق الفرد في الخصوصية ومنه ما تعلق بسرية مراسلاته واتصالاته وما يتفرع عنها كالمراسلات الإلكترونية، فهذا الحق مكفول دستوريا وفق نص المادتين (47-46) من القانون رقم:16-01 المؤرخ في:2016/03/06 يتضمن التعديل الدستوري ، لذا يجب أن يستخدم ضمن نطاق ضيّق وحينما تكون هناك خطورة محتملة على المصالح المحمية قانونا كما سنبيّنه لاحقا.

في هذا الصدد، نص المشرع الجزائري على هذا الإجراء بموجب المادة (03) من القانون 09-04 سالف الذكر، والتي تنص على: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية"، موافقا في ذلك نص المادة (21) من (إ.أ.م.إ.م) تحت عنوان "اعتراض معطيات المحتوى" والتي تؤكد على تجميع أو تسجيل في القوت الفعلي، المعطيات المتعلقة بمحتوى اتصالات معينة، منقولة عن طريق نظام معلوماتي[4]. وعليه فهو إجراء استثنائي لمساسه

---

[1] نايز نبيل عمر، المرجع السابق، ص149، راجع أيضا، عفيفي كامل عفيفي، المرجع السابق، ص ص474-475.

[2] نعيم سعيداني، المذكرة السابقة، ص183.

[3] نايز نبيل عمر، المرجع السابق، ص149.

[4] تنص المادة (21) من (إ.أ.م.إ.م) تحت عنوان: "اعتراض معطيات المحتوى" على:" يجب على كل طرف أن يتبنى الاجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة فيما يتعلق بالجرائم الخطيرة التي يحددها القانون الداخلي المكنات التالية:==

==أ- جمع أو تسجيل عن طريق تطبيق الوسائل الفنية المتواجدة على أرضه.

بالحق في سرية المراسلات بكافة أشكالها، كما أجازه المشرع في حالة وجود معلومات كافية عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، وهذا وفق نص المادة (04/ب) من القانون 09-04 سالف الذكر[1].

الفرع الثاني: حالات اللجوء للمراقبة الإلكترونية:

مما لاشك فيك أن مراقبة الأحاديث والاتصالات الخاصة والتي تتم بالوسائل الإلكترونية وعلى رأسها تقنية المعلومات خاصة في ظل الاستعمال الواسع لشبكة الإنترنت، تمسّ بحق الإنسان في الخصوصية المكفول دستوريا في مختلف التشريعات الحديثة، حيث أضحى هذا الحق تحت رحمة وتهديد تقنيات تنصت وتعقب حديثة تستعملها الدول تحت مبررات كثيرة، منها محاربة الإرهاب والحفاظ على الأمن القومي...إلخ، مما يفتح الباب واسعا للمساس بحرمة هذا الحق، لذا عمدت مختلف التشريعات إلى تحديد حالات على سبيل الحصر يجوز فيها مراقبة الاتصالات الإلكترونية للأفراد منعا للتعسّف في المساس بهذا الحق.

وعليه لم يترك المشرع الجزائري الأمر على إطلاقه استجابة للمواثيق الدولية وحماية لحقوق الإنسان في هذا المجال، حيث نصت المادة (04) من القانون 09-04 سالف الذكر على الحالات التي يجوز فيها مراقبة الاتصالات الإلكترونية حيث تنص على:" يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية:

أ- للوقاية من الأفعال الموصوفة بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني .

ج- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د- في اطار تنفيذ طلبات المساعدة القضائية الدولية.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة المختصة.

ب- إلزام مقدم الخدمات، في نطاق قدراته الفنية المتوافرة على :

ج- أن يجمع أو يسجل عن طريق تطبيق وسائل فنية موجودة على أرضه، أو أن يمنح السلطات المختصة عونه أو مساعدته من أجل تجميع أو تسجيل في القوت الفعلي، المعطيات المتعلقة بمحتوى اتصالات معينة على أرضه، منقولة عن طريق نظام معلوماتي...".

[1] المادة (04/ب) من القانون رقم:09 - 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

عندما يتعلق الأمر بالحالات المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه إذنا لمدة ستة(6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها".

يتضح لنا من نص هذه المادة أن المشرع الجزائري حدّد حالات اللّجوء للمراقبة الإلكترونية في بعض الجرائم على سبيل الحصر، ومنها الجرائم الإلكترونية بصفة عامة وجرائم المساس بأنظمة المعالجة الآلية للمعطيات بصفة خاصة، كما ربط ذلك بوجود ضرورة قصوى تدعو إليه تاركا تقديرها للجهة القضائية المختصة بمنح الإذن. حيث تنص المادة (04/ب-ج) على :"

ب- في حالة توفر معلومات عن احتمال اعتداء على معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ج- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللّجوء إلى المراقبة الإلكترونية...".

كما نستنتج من نص المادة السياسة الإجرائية الوقائية للمشرع الجزائري بخصوص مكافحة الجرائم الإلكترونية، رغم ما يترتب عن ذلك من المساس بحق الأشخاص في الخصوصية المحمي دستوريا، خاصة حينما يتم تطبيقه وفق مقتضيات النظام العام، الذي يظل مبهما وفضفاضا وغير محدد المعالم، مما قد ينجرّ عنه إخلال بشأن المساس بحقوق وحريات الأفراد[1]. لذا تفطن المشرع لذلك وأحاطه بجملة من الضوابط مثل: وجود ضرورة تدعو لهذا الإجراء وذلك في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[2] أو لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللّجوء إلى المراقبة الإلكترونية. كما أوجب المشرع تحت طائلة البطلان الحصول على إذن من السلطة القضائية المختصة لتنفيذ هذا الإجراء.

المطلب الثاني: شروط مراقبة الاتصالات الإلكترونية وكيفية القيام بها

[1] زيدان زيبحة، المرجع السابق، ص138.

[2] تبرز أمام الجزائر تحديات كبيرة في مجال مكافحة الجرائم الإلكترونية، خاصة في ظل توجهها نحو تحقيق متطلبات الحكومة الإلكترونية في مجالات عديدة، إضافة إلى إرساء القواعد المنظمة للتجارة الإلكترونية ، تجلت في الانطلاقة الرسمية للتعامل بأنظمة الدفع الإلكترونية ابتداء من:2016/10/04، مما يفتح أمام المجرم الإلكتروني مجالا جديدا وواسعا لارتكاب جرائمه.

نظرا لخطورة هذا الإجراء على حق الانسان في الخصوصية ومنها سريّة مراسلاته الإلكترونية أحاطه المشرع بضمانات قانونية تكفل عدم الاعتداء على هذه الحقوق، فما هي هذه الشروط؟ وكيف تتم هذه العملية؟، سنتناول شروط المراقبة الإلكترونية في (الفرع الأول)، ثم نتطرق إلى كيفية القيام بالمراقبة الإلكترونية في (الفرع الثاني).

الفرع الأول: شروط المراقبة الإلكترونية:

كما رأينا سلفا، وحفاظا على الحق في سريّة المراسلات بكافة أنواعها والمكفولة دستوريا، أحاط المشرع الجزائري إجراء المراقبة الإلكترونية تحت طائلة البطلان بشروط قانونية، تتمثل في النقاط الآتية:

أولا: وجود إذن قضائي: كما رأينا سلفا بخصوص أساليب التحرّي الخاصة والتي نص عليها المشرع الجزائري بموجب المادة(65 مكرر5 إلى المادة 65 مكرر18) من (ق.إ.ج.ج) تستوجب كلها الإذن القضائي سواء من طرف وكيل الجمهورية أو قاضي التحقيق، لأنها تمسّ بحرمة الحياة الخاصة للأشخاص، والأمر نفسه بالنسبة لإجراء المراقبة الإلكترونية على اعتبار أنها تمس أيضا بحق الأشخاص في سرية مراسلاتهم. أوجب المشرع أيضا وجود الإذن القضائي الصادر عن السلطة القضائية المختصة وذلك بموجب المادة (5/04) من القانون رقم: 09-04 سالف الذكر التي تنص على:"... لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية. عندما يتعلق الأمر بالحالات المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه إذنا لمدة ستة(6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها"[1].

كما حددت المادة نفسها الجهة القضائية المختصة بمنح الإذن في الحالة المنصوص عليها في (04/أ)، حينما يتعلق إجراء مراقبة الاتصالات الإلكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، في هذا الحالة يؤول الاختصاص إلى النائب العام لدى مجلس قضاء الجزائر بمنح الإذن لضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية

---

[1] تجيز بعض التشريعات الوطنية كالقانون الأمريكي وضع أجهزة لتسجيل الاتصالات الإلكترونية في حالة الضرورة دون إذن من النيابة العامة، إذا توافر خطر حال على الحياة أو خطر جسيم على السلامة الجسمية، خالد ممدوح ابراهيم، فن التحقيق، المرجع السابق ص351.

من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها[1].

أما فيما عدا هذه الحالة، يتعين الرجوع إلى التدابير التي رسمها (ق.إ.ج.ج) في مجال التحرّي والتفتيش بالنسبة للجرائم الإلكترونية، وبالضرورة في مجال الاختصاص بالنسبة لوكيل الجمهورية وكذا قاضي التحقيق باعتبارهما الجهة المؤهلة قانونا بمنح الإذن بالتفتيش، وذلك ما سنتناوله بالتفصيل في المبحث الثالث من هذا الفصل.

ثانيا: وجود ضرورة: قلنا سلفا أن هذا الإجراء استثنائي على عدم المساس بحق الشخص في الخصوصية ومنها سريّة المراسلات بكافة أشكالها، لذا يعتبر ضابط الوقاية السند والمبرّر الشرعي للقيام بمراقبة الاتصالات الإلكترونية، بالنسبة لمكافحة الجرائم الإلكترونية يتم اللّجوء إليه في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللّجوء إلى المراقبة الإلكترونية.

حيث يقصد بالمنظومة المعلوماتية وفق نص المادة (02/ب) من القانون رقم: 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، والملاحظ أن هذا التعريف يتفق مع نص المادة (01) من (إ.أ.م.إ.م) إذ تنص على:" يعتبر النظام المعلوماتي جهازا يتكوّن من معدات وبرامج قائمة للمعالجة الآلية للبيانات الرقمية...يمكن أن تكون منفردة أو متصلة مع أجهزة مماثلة أخرى داخل شبكة..."

فإذا تناهت إلى أسماع الجهات المختصة أن هناك احتمالا للاعتداء على منظومة معلوماتية ينتج عنه تهديد للنظام العام المتمثل أساسا في مجموعة الأسس السياسية والاجتماعية والاقتصادية والخلقية التي يقوم عليها كيان المجتمع، أو مؤسسات الدفاع الوطني كمؤسسة الجيش الوطني الشعبي، أو المؤسسات السيادية للدولة بقصد اختراقها للحصول على البيانات الحساسة سواء ما تعلق بالأفراد أو المؤسسات، خاصة في ظل اتجاه الدولة إلى رقمنه الإدارة تمهيدا لإرساء دعائم الحكومة الإلكترونية مثل: استخراج بعض الوثائق من الجهاز القضائي، واستخراج جواز السفر البيومتري وبطاقة التعريف البيومترية...إلخ. أو بهدف تخريب منظومة الاقتصاد الوطني، أو لمجريات التحقيقات

[1] المادة (6/04) من القانون رقم:09 – 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

القضائية حينما يتطلب كشف الحقيقة. أجاز المشرع استعمال المراقبة الإلكترونية للوقاية من الجرائم الإلكترونية للحد من أضرارها بما يخدم مصلحة الأفراد والدولة على حد سواء.

ثالثا: استخدام هذا الإجراء ضمن نطاق ضيق: نظرا لخطورة هذا الاجراء للأسباب المبينة سلفا، حدد المشرع الجزائري على سبيل الحصر -كما رأينا سلفا- حالات اللّجوء إليه إضافة إلى أنه يتم بإذن قضائي، فمن جهة ضمانا لحقوق وحريات الأفراد المكفولة دستوريا، ومن جهة أخرى مراعاة لحق المجتمع في الدفاع عن نفسه ضد الجريمة والوقاية منها.

من ناحية أخرى أدت أسباب كثيرة لفرض هذا الإجراء الاستثنائي على الحق في الخصوصية منها:

- كثرة جرائم الاعتداء على المنظومات المعلوماتية التي يعتبرها قراصنة المعلوماتية بنوكا ثمينة بما تحتويه من معلومات وبيانات سواء ما تعلق بالأفراد أو الشركات أو مؤسسات الدولة، بما يهدد الأمن القومي الوطني.

- ازدياد اعتماد المجرمين المعلوماتيين على تقنية المعلومات واستعمالها للاعتداء على المجالات الحيوية المرتبطة ارتباطا وثيقا بكيان الدولة وأمنها وسلامة اقتصادها، مثل: جريمة الدخول غير المشروع في منظومة معلوماتية والتلاعب في البيانات والمعلومات التي تحتويها بقصد استغلالها بما يؤثر على أمن الأفراد والدولة على حد سواء.

كما تجدر الإشارة إلى أن المشرع ترك السلطة التقديرية لتقدير حالة الضرورة للّجوء لهذا الإجراء، للسلطة القضائية صاحبة الاختصاص في منح الإذن، حيث يمكن لها قبول أو رفض هذا الإجراء تبعا لفائدته من عدمها في الوصول إلى كشف المجرم الإلكتروني، نظرا لخطورته ومساسه بخصوصية الأفراد المحمية قانونا.

الفرع الثاني: كيفية القيام بها:

بعد تحقّق قيام إحدى حالات المراقبة الإلكترونية المنصوص عليها قانونا، وبعد الحصول على الإذن من الجهة القضائية المختصة، تتم عملية مراقبة الاتصالات الإلكترونية وفق المراحل الآتية:

أولا: وضع الترتيبات التقنية اللاّزمة: إن التقنية المستعملة في مراقبة الاتصالات الإلكترونية هي التقنية الإلكترونية والتي مفادها:" مجموعة الأجهزة المتكاملة مع بعضها بغرض تشغيل مجموعة من البيانات الداخلة وفقا لبرنامج موضوع مسبقا للحصول على النتائج المطلوبة"[1]، كما نجد من بين

---

[1] مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنيت-دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكتاب الخامس، دار الكتب والوثائق القومية المصرية، مصر، ط1، 2003، ص205.

التقنيات المستعملة في المراقبة الإلكترونية برنامج *(CARNIVORE)*[1] أو (آكل البيانات) الذي له الأثر الفعّال في الرصد المبكر للاعتداءات المحتملة، أو تقنية مراقبة البريد الالكتروني*(e-mail)*[2] بالرغم أن بعضا من الفقه يرى أن المراقبة البرمجية لاتزال محل نظر، من حيث ضرورة الالتزام بما هو مقرر قانونا، ضمانا لعدم المساس بالحق في الخصوصية المكفول دستوريا. ذلك أن إعداد برمجيات تتولى بذاتها البحث عن الجرائم ومرتكبيها مثل: برنامج *(carnivore)*، أمر قد لا يتوافق مع الضمانات الدستورية المعاصرة، لما يشكله مثل هذا الإجراء من عدوان على الحق في الخصوصية والذي يعد أقوى مظاهر الحقوق الدستورية الفردية[3].

بعد توفر الشروط اللاّزمة للقيام بعملية مراقبة الاتصالات الإلكترونية خاصة وجود الإذن القضائي، تقوم الجهات المعنية بعملية مراقبة الاتصالات الإلكترونية عن طريق الفنيين التابعين لها بوضع الترتيبات التقنية اللاّزمة بهدف تجميع وتسجيل محتواها في حينها، وتتمثل هذه الجهات المعنية في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي من مهامها ضمان المراقبة الوقائية للاتصالات الإلكترونية بغرض الكشف عن الأعمال الإرهابية والتخريبية، والمساس بأمن الدولة تحت سلطة القاضي المختص وذلك وفقا لنص (6/04) من القانون رقم:09-04 سالف الذكر، إضافة إلى السلطات القضائية المكلفة بالبحث والتحري في حالة توفرها على معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع

---

[1] برنامج: *(CARNIVORE)*:هو نظام كومبيوتري مصمّم ليسمح لوكالة المباحث الفيدرالية الأمريكية *(F.B.I)*، وبالتعاون مع الشركة المزودة لخدمات الإنترنت، وذلك من أجل تعقب وفحص رسائل البريد الإلكتروني المرسلة والواردة عبر أي حساب خادم تستخدمه أي شركة تقوم بتوفير خدمة الإنترنت، ويشتبه في أن تيار الرسائل المار عبر خدماتها يحمل معلومات عن جرائم جنائية. حيث يتم تنفيذ عمليات التعقب والفحص بوضع أجهزة الشركة الموفرة للخدمة تحت المراقبة الإلكترونية . وقد حقّقت هذه التقنية نجاحا كبيرا في تعقب المجرمين، حيث أصبح يطلق على هذه التقنية بعد أحداث 11سبتمبر 2001 تقنية (*dcs* 1000)، وأصبحت تختص بمتابعة القضايا المتعلقة بالأمن القومي الأمريكي والتصدي لأي هجومات محتملة في المستقبل. كما يمكن استخدام نظام *(CARNIVORE)* بشكلين فقط الأول: هو رصد المعلومات الواردة والصادرة من وإلى حساب بريد إلكتروني معين*(e-mail)*، أو رصد حركة البيانات من وإلى عنوان *(IP)* معين. ويتم ذلك بعدة طرق، وذلك إما من خلال رصد جميع الترويسات *(headers)* الخاصة برسائل البريد الإلكتروني (بما في ذلك عناوين البريد الإلكتروني) الصادرة من والواردة إلى حساب معين، والطريقة الثانية: هي رصد جميع الأجهزة المزودة (مزودات الويب، والملفات) التي يقوم المشتبه به بالنفاذ إليها، كما يوجد هناك برنامج آخر يسمى(بورنزويبر) مهمته الرقابة على الصور المرفقة برسائل البريد الإلكتروني، مصطفى محمد موسى، المراقبة الالكترونية ، المرجع نفسه، ص ص208-210، راجع أيضا، فايز محمد راجح غلاب، الأطروحة السابقة، ص353.

[2] تقنية مراقبة البريد الإلكتروني: عبارة عن برنامج صممه الأمريكي (ريتشارد أتوني) من أجل سبر محتوى البريد الإلكتروني موضوع المراقبة وقراءة الرسائل التي قام صاحبها بإتلافها أو تلك التي لم يقم بتخزينها. حيث استخدمت أجهزة الاستخبارات الأمريكية هذا البرنامج من أجل كشف مشتبه فيه من الجنسية الروسية حاول اختراق مواقع على شبكة الإنترنت، مصطفى محمد موسى، المراقبة الإلكترونية المرجع السابق، ص214 وما بعدها.

[3] عمر محمد أبو بكر بن يونس، الرسالة السابقة، ص840.

الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو لمقتضيات حماية النظام العام أو لمستلزمات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الابحاث الجارية دون اللّجوء إلى المراقبة الإلكترونية.

ثانيا: تجميع الاتصالات الإلكترونية وتسجيل محتواها: من الملاحظ أن هناك تشابها كبيرا بين الرسالة الإلكترونية والرسالة الورقية، حيث عرّف المشرع الجزائري البريد الإلكتروني بموجب المادة (2/02) من المرسوم التنفيذي رقم:98-257 المؤرخ في:1989/08/25 يضبط شروط وكيفيات إقامة خدمات انترنات واستغلالها على أنه: "خدمة تبادل رسائل إلكترونية بين المستعملين"[1] فالبريد الإلكتروني*(E.MAIL)* يحتوي على برامج متخصصة لكتابة وإرسال واستقبال واستعراض وتخزين الرسائل الإلكترونية[2]، كما أن التعامل مع الرسائل الإلكترونية لا يختلف في مضمونه عن التعامل مع الرسائل الورقية إلا من حيث الوسيلة المستخدمة، حيث يكون بمقدور المستخدم عدم الرد عليها أو طبعها أو حفظها في ملف خاص[3].

حيث يتم تجميع وتسجيل محتوى الاتصالات الإلكترونية التي تتم بكل وسيلة إلكترونية على وسائط تخزين معلوماتية مثل: القرص الصلب، أو القرص المضغوط أو الذاكرة الوميضية...إلخ خاصة تلك الاتصالات التي تتم على شبكة الإنترنت باستعمال برامج متخصصة، أو التي تتم باستعمال الهاتف الذكي المزوّد بشريحة يمكن من خلالها الاتصال بشبكة الإنترنت ونقل الاتصال بالصوت والصورة بواسطة برامج متخصصة مثل: برنامج(*Messenger,Skype,WhatsApp... ...)*، أو التي تتم بواسطة البريد الإلكتروني.

من جانب آخر يمكن تطبيق المراقبة الإلكترونية على شبكات الحاسوب بالنسبة للمحادثات التي تتم عبره بواسطة شبكة الإنترنت والتي تستعمل برامج عديدة مثل: سكايب *(Skype)* وميسنجر*(Messenger)*، ناهيك عن وسائل التواصل الاجتماعي عبر الإنترنت مثل: تويتر وفايسبوك *(Facebook,Twitter)* التي توفر هذه الخدمة، طالما أن النتيجة واحدة وهي سماع تلك

---

[1] المادة (2/02) من المرسوم التنفيذي رقم:98-257 المؤرخ في:1989/08/25 يضبط شروط وكيفيات إقامة خدمات انترنات واستغلالها، (ج.ر) رقم:63 المؤرخة في:1989/09/26، ص6.

[2] كما يعرف البريد الإلكتروني أيضا على أنه:" تبادل الرسائل والوثائق باستخدام الحاسب الآلي"، إذا تتم عملية إرسال واستقبال البريد الإلكتروني بواسطة مقدم خدمة الإنترنت، والذي يتولى تقديم هذه الخدمة من المرسل إلى المرسل إليه والعكس، وحتى تتم الخدمة لا بد من توافر معلومات مثل: اسم مزود إرسال البريد الالكتروني ويرمز له *(SMTP)*، اسم مزود استقبال البريد الالكتروني *(POP)*، عنوان البريد الإلكتروني للمستخدم في شبكة الانترنيت...إلخ، راجع عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص792.

[3] فايز محمد راجح غلاب، الأطروحة السابقة، ص354.

المحادثات وتسجيل محتواها في حينها والاحتفاظ بها كدليل على وقوع الجريمة أو الوقاية منها. إن الأهم هنا هو مراعاة شروط المراقبة الإلكترونية بما يحفظ الحق في الخصوصية ولا يتعارض مع تحقيق العدالة[1].

تتم عملية مراقبة الاتصالات الإلكترونية باستعمال وسائل تقنية متطورة بما يستوجب على الدولة تجهيز السلطات القضائية المختصة بالبحث والتحري، وكذا الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بالوسائل التقنية اللاّزمة، ناهيك عن تدريب أفرادهما على استعمالها لإكسابهم المهارة المطلوبة للبحث والتحري عن الجرائم الإلكترونية.

المطلب الثالث: التزامات مقدمي الخدمات

نظرا لخصائص الدليل الرقمي في الجريمة الإلكترونية الموجود أساسا ضمن بيئة افتراضية، مما يخلق صعوبات بالغة للسلطات القضائية المكلفة بالبحث والتحري لاستخلاصه، فإن المجرم المعلوماتي يستعمل التقنية المعلوماتية ذاتها في ارتكاب جريمته والتهرب من الملاحقة، فهو يستطيع في وقت يسير جدا، إخفاء الدليل الإلكتروني أو محوه أو تعديله...إلخ. مما يطرح الحاجة إلى وضع إطار قانوني يلزم فيه المشرع مقدمي الخدمات بضرورة أرشفة الاتصالات والمراسلات الإلكترونية لاستعمالها عند الحاجة إليها في مجال التحريات والتحقيقات القضائية، أو في مجال الوقاية من الجرائم الإلكترونية، وهذا ما تضمنه قرار الجمعية العامة للأمم المتحدة رقم:(63/55) بتاريخ:2001/01/22 والمتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية وذلك بموجب المادة (01/و) منه والتي ألزمت فيها الدول أن تسمح بحفظ المعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية الخاصة وسرعة الحصول عليها[2]، وهذا ما نص عليه المشرع الجزائري بموجب المادتين (10-11) تحت عنوان: "التزامات مقدمي الخدمات".

سنتطرق إلى مفهوم مزودي الخدمات في (الفرع الأول)، ثم نتناول الالتزامات الملقاة على عاتقهم في (الفرع الثاني).

---

[1] الأطروحة نفسها، ص357.

[2] قرار الجمعية العامة للأمم المتحدة رقم:(63/55) بتاريخ:2001/01/22 والمتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، متوفر على الموقع الرسمي للأمم المتحدة على الرابط الآتي:
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/55/63،تاريخ الاطلاع:2016/04/15 على الساعة:09:31.

الفرع الأول: مفهوم مقدمي الخدمات:

عرفت (إ.أ.م.إ.م) مقدمي الخدمات بموجب المادة (01/ج) التي تنص على:" يقصد بمزودي الخدمات:

– أيٌّ كيان عام أو خاص الذي يوفر لمستخدميه القدرة على التواصل من خلال النظام المعلوماتي.

– أيٌّ كيان آخر يقوم بمعالجة أو تخزين البيانات الحاسوبية لخدمة الاتصالات أو لخدمة مستخدميه..."[1].

وهو التعريف نفسه الذي خص به المشرع الجزائري مقدمي الخدمات بموجب المادة (02/د) من القانون رقم:09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الإتصال ومكافحتها التي تنص على:" يقصد في مفهوم هذا القانون ما يأتي...:

د– مقدمو الخدمات:

– أيٌّ كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام اتصالات.

– وأيٌّ كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها".

إن مزود خدمة الإنترنت *(ISP)* هو اختصار لكلمة *(Internet Service Provider)* ويسمى أيضا بموفر خدمة الاتصال بالإنترنت *(AIP)*، هي الشركة التي توفر لعملائها إمكانية الوصول إلى الإنترنت. ويرتبط مزود خدمة الإنترنت بعملائه باستخدام تقنية نقل البيانات المناسبة لتوصيل حزم بيانات نظام الإنترنت، مثل: الاتصال الهاتفي، خط المشترك الرقمي للاتصال*(DSL)* كابل المودم، لاسلكية الوصلات المخصصة عالية السرعة...إلخ. إن مزود خدمة الإنترنت قد يوفر

---

[1] ***Article 1 – Définitions***

Aux fins de la présente Convention, l'expression…

c.«fournisseur de service» désigne :

i. Toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;

ii. Toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs, convention européenne de la cybercriminalité, Op.Cit,p.3.

حسابات البريد الإلكتروني للمستخدمين، والتي تسمح لهم بالتواصل مع بعضهم البعض عن طريق إرسال واستقبال الرسائل الإلكترونية من خلال خادم*(server)* مزود خدمة الإنترنت(وكجزء من خدمة البريد الإلكتروني عادة ما يوفر مزود خدمات الإنترنت للمستخدم وعميل البريد الإلكتروني حزمة البرامج، التي طُورت داخليا أو من خلال ترتيب عقد خارجي، كما يمكن لمقدمي خدمات الإنترنت توفير خدمات أخرى مثل: تخزين البيانات عن بعد نيابة عن عملائها[1].

من جانب آخر هناك أيضا ما يعرف بمتعهد الإيواء أو استضافة الويب *(web hosting)* وقد يكون شخصا طبيعيا أو معنويا يقوم بتوفير خدمات الاتصال على الخط أو تخزين الإشارات والبيانات والصور...إلخ[2]. كما يقوم أيضا بتخزين البرامج التطبيقية والملفات الخاصة بالزبائن وضمان خدمة النفاذ لشبكة الإنترنت 24/24 ساعة[3].

إن مواقع الإنترنت ما هي إلا اسم نطاق أو دومين وهو اسم أو عنوان الموقع الذي ينقل المتصفح إلي الموقع المطلوب، وهذا الموقع يحتوي على صور وكتابات ومواد هي الأخرى بدورها ينبغي أن تكون على خادم، حيث يربط النطاق الخاص بهذا الموقع بعنوان الخادم *(IP)* . ويمكن تقسيم أنواع الاستضافة إلى استضافة مجانية وأخرى مدفوعة، حيث تتجه بعض الشركات إلى تقديم خدمة الاستضافة المجانية في مقابل الحصول على خدمات خاصة مثل: الإعلان على المواقع المستضيفة لديها[4].

من جانب آخر يتجه كثير من الشركات والأفراد إلى استضافة مواقعهم على خوادم مجانية وبذلك يتنازلون عن جملة من المزايا في مقابل هذه المجانية، حيث صار التوجه هذه الأيام إلى الاستضافة المجانية بسيطا جدًا لا يكاد يذكر إلا من بعض الأفراد القلائل وفي المواقع الشخصية الصغيرة فقط على الأغلب، والسبب في ذلك انخفاض تكاليف الاستضافات المدفوعة بنسبة كبيرة مقارنة بالفترات السابقة مما يغري أصحاب المواقع بالتمتع بالمزايا العديدة التي يحصلون عليها مع الاستضافات المدفوعة[5].

---

[1] عبد الفتاح بيومي حجازي، الجرائم المستحدثة، المرجع السابق، ص92.

[2] *Quéméner(Myriam) et Charpenel (Yves),Op.Cit,pp.40-41.*

[3] *CHRISTIANE FERAL-SCHUHL, Le Droit à L'épreuve , 2e édition, Op.Cit,p.122.*

[4] *Mohammed Buzubar, art-Cit,pp.56-57.*

[5] عبد الفتاح بيومي حجازي، الجرائم المستحدثة، المرجع السابق، ص93، راجع أيضا، زيدان زيبحة، المرجع السابق، ص ص154-155.

وعليه فإن المراسلات التي تتم بواسطة البريد الالكتروني والتي يتم استقبالها بواسطة مزود الخدمة[1] الخاص بالمرسل إليه والتي لم يطلع عليها بعد، فإنها تستقر في حالة تخزين إلكتروني كإجراء مؤقت في انتظار استقبال المرسل إليه لها من مزود الخدمة، وبمجرد استقبال المرسل إليه الخدمة فإن مزود الخدمة إما يقوم بمسح تلك الرسالة أو يقوم بتخزينها[2].

إن مزود الخدمة يمكنه أن يكشف كل أفعال مستخدم الإنترنت عندما يتصل بالشبكة، ويندرج تحت هذه الأفعال المواقع التي زارها وتاريخ الزيارة والصفحات التي اطلع عليها والملفات التي خزّنها والكلمات التي بحث عنها، وكذلك الحوارات التي أجراها وحركة البريد الإلكتروني الخاصة به من إرسال واستقبال وفواتير الشراء والخدمات التي اشترك فيها...إلخ، وفي كل الأحوال يتوقف جمع هذه المعلومات على الوسائل التقنية المستعملة. وبمعنى آخر لو كان مزود الخدمة يحق له مراقبة العملاء والذي يتم عادة في إطار مشروع، فسيتمكن من جمع المعلومات التي يريدها، فضلا عن إمداد الجهات الرسمية والقضائية بالمعلومات التي يريدها[3]، ويدخل هذا في إطار مساعدة السلطات القضائية. وهو ما أقره المشرع الجزائري بموجب نص المادة (10) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الإتصال ومكافحتها لتسهيل مكافحة الجرائم الإلكترونية.

أما بخصوص قطاع الاتصالات في الجزائر فتهيمن عليه ثلاث شركات كبرى، الأولى شركة "اتصالات الجزائر" وهي الشركة الأم والتي تقدم خدمات الاتصالات الهاتفية الثابتة والمحمولة ولكنها لم تكن الشركة الأولى التي قدمت خدمات الهاتف المحمول حيث حصلت شركة" أوراسكوم تيليكوم" المصرية على أول رخصة تشغيل الهاتف المحمول في الجزائر عبر شركتها "جيزي"، قبل أن تطلق اتصالات الجزائر شركتها "موبيليس"، وأخيرا شركة الوطنية الكويتية كمُشغّل ثالث من خلال شركة" نجمة" ثم غيّرت التسمية إلى "أوريدو"، يخضعون في أنشطتهم إلى دفتر الشروط المحدد من قبل

---

[1] من أشهر مزوّدي خدمة البريد الالكتروني نجد: *(Gmail) (Yahoo) (Hotmail) (out look express) (maktoob)*، حيث تتنافس فيما بينها حول الخدمات المقدمة مثل: المساحة المتوفرة وحجم الرسائل المراد إرسالها وتصفية الرسائل المزعجة وفحص مرفقات الرسائل لضمان خلوها من الفيروسات...إلخ.

[2] رشيدة بوكر، المرجع السابق، ص447.

[3] عبد الفتاح بيومي حجازي، الجرائم المستحدثة، المرجع السابق، ص92، راجع أيضا، *CHRISTIANE FERAL-SCHUHL, Le Droit à L'épreuve, 2e édition, Op.Cit,pp.131-132.*

سلطة الضبط للبريد والمواصلات السلكية واللاّسلكية، إضافة إلى عدد كبير من مزودي خدمة الإنترنت[1].

الفرع الثاني: التزامات مقدمي الخدمات ومسؤوليتهم:

نظرا لأهمية الدور الفعّال الذي يلعبه مقدمو الخدمات في مكافحة الجرائم الإلكترونية عن طريق تسهيل الوصول إلى الأدلة الرقمية، رأى المشرع أنه من الضروري إلزام الأطراف المتدخلة في توفير الخدمات، بتقديم المساعدات الضرورية للجهات القضائية المكلفة بالتحريات والتحقيقات وذلك تطبيقا لنص المادة (23) من (إ.ع.م.ج.ت.م) تحت عنوان:" التحفظ العاجل على البيانات المخزنة في تقنية المعلومات" التي أجبرت الدول الأطراف على تبني الإجراءات الضرورية لتمكين السلطات المختصة من الحصول العاجل على المعلومات المخزنة وإصدار الأمر إلى شخص من أجل حفظ المعلومات المخزنة والموجودة بحيازته ومن أجل إلزامه بحفظ وصيانة تلك المعلومات[2].

وعليه نص المشرع الجزائري بموجب المادتين (10-11) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الإتصال ومكافحتها على الالتزامات الملقاة على عاتقهم، والمتمثلة في مساعدة السلطات القضائية وحفظ المعطيات المتعلقة بحركة السير وذلك تحت طائلة العقوبات الإدارية والجزائية في حالة الإخلال بها.

---

[1] تم إنشاء سلطة الضبط للبريد والمواصلات السّلكية واللاّسلكية بموجب المادة (10) من القانون رقم: 2000-03 المؤرخ في الخامس أوت 2000 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السّلكية واللاّسلكية، وذلك في إطار تحرير سوق البريد والمواصلات السّلكية واللاّسلكية. واخضاعه للمنافسة عن طريق تشجيع مشاركة الاستثمار الخاص في هذه الأسواق، من بين مهامها:

- منح تصريحات التشغيل واعتماد معدات البريد والاتصالات السّلكية واللاّسلكية ووضع المواصفات والمعايير التي يجب أن تستجيب لها.
- تحديد قواعد لمتعاملي شبكات الاتصالات العامة بهدف تسعير الخدمات المقدمة للجمهور.
- إجراء مناقصة لمنح تراخيص إنشاء وتشغيل شبكات الاتصالات العامة التي تخضع لنظام الترخيص.

أكثر تفاصيل، يرجى الاطلاع على الموقع الرسمي لسلطة الضبط للبريد والمواصلات السلكية واللاسلكية: *http://www.arpt.dz/ar/arpt/bref/*، تاريخ الاطلاع: 2016/04/15 على الساعة:16:53.

[2] تنص المادة (23) من (إ.ع.م.ج.ت.م) على:

"1-تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين، والتي خُزّنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة(1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوما قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي.

3- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية المعلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي".

أولا: مساعدة السلطات القضائية: تنص المادة (10) من القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على: "في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه تحت تصرف السلطات المذكورة. ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق".

وعليه ألزم المشرع مزوّدي الخدمات بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات الملزمين بحفظها. وتشمل هذه المساعدة المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وتلك المتعلقة بالتجهيزات المستعملة في الاتصال، والخصائص التقنية وتاريخ وزمن ومدة كل اتصال، والمعطيات المتصلة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، بالإضافة إلى المعلومات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وعناوين المواقع المطلع عليها...إلخ.

وحسنا فعل المشرع، لأن هذا الأمر يُسهل إلى حد كبير من مهمة أجهزة البحث والتحري لكشف الجريمة وملاحقة المجرم المعلوماتي في هذه البيئة الافتراضية.

ثانيا: حفظ المعطيات المتعلقة بحركة السير: من نصوص المواد سالفة الذكر يُفهم أن حفظ المعطيات تتعلق بقيام مزود الخدمة بتجميع المعطيات المعلوماتية وتسجيلها في حينها وحفظها ضمن أوعية التخزين والاحتفاظ بها في المستقبل لأجل مقتضيات التحريات والتحقيقات القضائية كإجراء التفتيش مثلا. والمعطيات المقصودة هنا هي تلك التي نص عليها المشرع بموجب (02/هـ) من القانون رقم: 09-04 المؤرخ في 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والمتمثلة في:" أيُّ معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة. وهو ما تشير إليه أيضا نص المادة (16) من (إ.أ.م.إ.م) التي تنص على شمول المعطيات المتعلقة بحركة السير بإجراء الحفظ[1].

---

[1] ***Article 16 – Conservation rapide de données informatiques stockées***

"Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la==

في هذا الشأن أيضا، حدد المشرع الجزائري بموجب المادة (11) من القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المعطيات المتعلقة بحركة السير والتي تخضع لنظام قانوني واحد بما يعني التزام مزود الخدمة بحفظها، حيث تنص المادة (11) على:" مع مراعاة طبيعة ونوعية الخدمات يلتزم مقدمو الخدمات بحفظ:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة،
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها،

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة(أ) من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه..." وهي التزامات مقدمي الخدمات التي نصت عليها المادة (28) من (إ.ع.م.ج.ت.م) تحت عنوان: "الجمع الفوري لمعلومات تتبع المستخدمين"[1].

مما لاشك فيه أن حفظ هذه المعطيات يشكل بنكا من المعلومات الهامة لمساعدة السلطات القضائية المكلفة بالبحث والتحري في الجرائم الإلكترونية للكشف عن المجرم الإلكتروني واقتفاء آثاره

==conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification ..."convention européenne de la cybercriminalité, Op.Cit,pp.8-9.

[1] حيث تنص المادة (28) من (إ.ع.م.ج.ت.م) على:" تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من:

أ- جمع أو تسجيل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف،

ب- الزام مزود الخدمة ضمن اخصاصه الفني بأن:

- يجمع أو يسجل بواسطة الوسائل الفنية على إقليم الدولة الطرف، أو
- يتعاون ويساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

2-إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة(1-أ) فيمكنها تبني إجراءات أخرى بالشكل الضروري الجمع أو التسجيل الفوري لمعلومات تتبع المستخدمين المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام مزود الخدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة".

لأنه يصعب عليه من الناحية الفنية اختراق هذه الأنظمة، مثل: أنظمة شبكة الاتصال المتعلقة بالهاتف النقال، قصد محو المعطيات المتعلقة باتصالاته سواء في حال كان هو المرسل أو كان هو المرسل إليه، من جهة أخرى حدد المشرع مدة حفظ المعطيات بسنة واحدة، وذلك بموجب نص المادة (7/11) من القانون 09-04 التي تنص على: "تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل..."، وهي مدة معقولة جدا أكثر مما نصت عليه المادة (23) من (إ.ع.م.ج.ت.م)، حيث حددتها بتسعين (90) يوما قابلة للتجديد، حيث تسمح مدة سنة لأجهزة البحث والتحري بالرجوع إلى هذه المعطيات في حال وقوع جريمة، بما لا يسمح للمجرم الإلكتروني الإفلات من العقاب.

ثالثا: مسؤولية مقدمي الخدمات: مما سبق ذكره عرفنا أن مقدمي الخدمات يقومون بدور فني بحت يتمثل في توصيل الزبون إلى شبكة الخدمة ولا علاقة لهم بمحتوى المادة التي ينشرها الزبون .

بالنسبة للمشرع الجزائري نص في المادة (11) من القانون 09-04 سالف الذكر على:" دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة(6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000دج إلى 500.000دج . يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات".

من جهة أخرى، ألزم المشرع الجزائري مزودي الخدمات تحت طائلة العقوبات كتمان سرية العمليات التي ينجزونها، وذلك وفق نص المادة (2/10) من القانون 09-04 سالف الذكر والتي تنص على: "يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق".

وعليه فرض المشرع الجزائري على مزوّدي الخدمات سواء كانوا أشخاصا طبيعيين أو معنويين عقوبات إدارية وجزائية في حالة الإخلال بالتزاماتهم وأدت إلى عرقلة حسن سير التحريات القضائية أو إفشاء للغير سرّية العمليات التي يقومون بها بمناسبة التحريات بخصوص جريمة ما[1]، وحسنا فعل المشرع فعدم التزام مزوّدي الخدمات يؤدي إلى ضياع الدليل الرقمي واختفاء آثار الجريمة في هذا الوسط الافتراضي مما يكرّس سياسة اللاّعقاب.

---

[1] المادتان (302-301) من (ق.ع.ج).

المطلب الرابع: الالتزامات الخاصة بمقدمي خدمة الإنترنت ومسؤوليتهم

فرضت التكنولوجيا الحديثة في مجال تقنية الحوسبة والاتصال وكذا الانتشار الواسع لشبكة الإنترنت والتحديات التي يفرضها مجتمع المعلومات خاصة ما تعلق بإساءة استخدام هذا العالم الافتراضي إلى تدخل المشرع الجزائري لتنظيمه وتحديد مسؤولية المتدخلين في هذا المجال الحيوي فلم يكتف المشرع بالنص على التزامات مزودي الخدمات فقط، بل نص أيضا على التزامات خاصة بمقدمي خدمة الإنترنت، سنتناول مفهوم مقدمي خدمة الإنترنت في(الفرع الأول)، ثم نتطرق إلى التزاماتهم ومسؤوليتهم في (الفرع الثاني).

الفرع الأول: مفهوم مقدمي خدمة الإنترنت:

تطرقنا سابقا إلى مفهوم مقدمي الخدمات وهو التعريف الذي جاء به نص المادة (02/د) من القانون رقم:09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تنص على:" يقصد في مفهوم هذا القانون ما يأتي...:

د- مقدمو الخدمات:

- أيُّ كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام اتصالات.

- وأيُّ كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها".

وعليه يدخل ضمن هذا التعريف مقدمو خدمة النفاذ لشبكة الإنترنت *(Internet Service Provider)*، حيث تتعدد طرق النفاذ إلى شبكة الإنترنت مثل: خط اشتراك رقمي غير متماثل *(ADSL)...إلخ*، إلا أنه في كل الأحول يجب وجود مقدم خدمة الإنترنت *(Internet Service Provider)* الذي يعرف على أنه: "الشركة التي تستضيف مواقع الإنترنت على خوادمها*(Servers)* حيث يكون مقدم الخدمة مؤجرا وصاحب الموقع مستأجرا ويسمى أيضا" بموفر خدمة الاتصال بالإنترنت" *(AIP)*[(1)] ، وهي الشركة التي توفر لعملائها إمكانية الوصول إلى الإنترنت. ويرتبط مزود خدمة الإنترنت بعملائه باستخدام تقنية نقل البيانات المناسبة لتوصيل حزم بيانات نظام الإنترنت مثل: الاتصال الهاتفي، كابل المودم...إلخ[(2)]. كما أن مزودي خدمة الإنترنت لا يجبرون على مراقبة المحتوى[(3)].

---

[1] *Quéméner(Myriam) et Charpenel (Yves),Op.Cit,p.38.*

[2] *Quéméner(Myriam) et Charpenel (Yves),Ibid,p.38.*

[3] *Quéméner (Myriam) et Ferry (Joel), Op.Cit,p.53.*

من جهة أخرى، يوفر مزود خدمة الإنترنت حسابات البريد الإلكتروني للمستخدمين، والتي تسمح لهم بالتواصل مع بعضهم البعض عن طريق إرسال واستقبال الرسائل الإلكترونية من خلال خادم*(server)* مزود خدمة الإنترنت(وكجزء من خدمة البريد الإلكتروني عادة ما يوفر مزود خدمات الإنترنت للمستخدم وعميل البريد الإلكتروني حزمة البرامج، كما يمكن توفير خدمات أخرى مثل: تخزين المعطيات عن بعد نيابة عن زبائنها[1].

بالنسبة للجزائر ومع التطور السريع الحاصل في مجال استغلال وتوسيع شبكة الإنترنت، ومع دخول خدمة الجيل الرابع *(4G)* حيث بلغت نسبة الاتصال بشبكة الإنترنت 26 %خلال سنة 2014، أي ما يعادل 26 جزائري من أصل 100 متصلون بشبكة الإنترنت[2]، حيث منحت سلطة الضبط للبريد والمواصلات السّلكية واللاّسلكية تراخيص لعدد كبير من مزودي خدمة الإنترنت لتغطية الطلب المتزايد على خدمات الشبكة العنكبوتية[3]، حيث يمكن للمستخدم الولوج لشبكة الإنترنت والاستفادة من خدماتها، وعليه فبإمكان مزود خدمة الإنترنت الاطلاع على جميع الخطوات التي قام بها المستخدم مثل: المواقع التي زارها مع تحديد تاريخ الزيارة ومدتها ووقتها والمعلومات التي خزنها والاتصالات التي أجراها...إلخ، وهو ما يمثل مراقبة للنظام دون إذن قضائي[4].

الفرع الثاني: التزامات مقدمي خدمة الإنترنت ومسؤوليتهم:

فرض المشرع الجزائري التزامات على عاتق مزودي خدمة الإنترنت، ينجّر عنها تحمّل مسؤوليتهم في حال الإخلال بها، وذلك نظرا لحساسية هذا القطاع بالنسبة للدولة والمواطن على حد سواء، وما يشكله أيضا من بيئة خصبة لانتشار الجرائم الإلكترونية.

---

[1] عماد مجدي عبد الملك، المرجع السابق، ص39-40، راجع أيضا، و *CHRISTIANE FERAL-SCHUHL, Le Droit à L'épreuve, 2e édition, Op.Cit,p.127.*

[2] تقرير نشاطات سلطة الضبط للبريد والمواصلات السّلكية واللاّسلكية لسنة 2014، منشور على الموقع الرسمي لسلطة الضبط على الرابط الآتي:*http://www.arpt.dz/ar/pub/raa* ، تاريخ الاطلاع:15/04/2016 على الساعة:20 :17.

[3] حيث تحتوي القائمة المنشورة على الموقع الرسمي لسلطة الضبط للبريد والمواصلات السّلكية واللاّسلكية على 25 مُزوّد خدمة النفاذ لشبكة الإنترنت، لأكثر تفاصيل يرجى زيارة الموقع على الرابط الآتي:*http://www.arpt.dz/ar/obs/prest/?c=fai* ، تاريخ الاطلاع:15/04/2016 على الساعة:17:23.

[4] في هذا الشأن يثار التساؤل حول مدى جواز قيام مزودي خدمات الإنترنت بمراقبة النظام دون إذن قضائي؟. حيث أجازت بعض التشريعات ومنها التشريع الأمريكي واعتبرته استثناء خاص بمزودي الخدمة، وذلك لمعرفة ما يقوم به المشتركون من إساءة الاستعمال مثل: نشاط التداخل مع أجهزة الآخرين أو تخزين مواد مخالفة للقانون أو الإضرار بالأجهزة باستعمال الفيروسات وانتهاك الحق في الخصوصية بواسطة الاختراق...إلخ، راجع، خالد ممدوح ابراهيم، فن التحقيق، المرجع السابق، ص ص356-357 .

أولا: التزامات مقدمي خدمة الإنترنت: في إطار تنظيم المشرع الجزائري لخدمة الإنترنت في الجزائر، أخضع مزودو هذه الخدمة لعدة التزامات، ضمانا لتقديم أحسن الخدمات وحفاظا على المجتمع من أخطار الإنترنت، في هذا الصدد نصت المادة (14) من المرسوم التنفيذي رقم:98-257 المؤرخ في:1998/08/25 يضبط شروط وكيفيات إقامة خدمات انترنات واستغلالها على:" يلتزم مقدم خدمة "انترنات" خلال ممارسة نشاطه بما يأتي:

- تسهيل النفاذ إلى خدمات انترنات، حسب الإمكانيات المتوفرة إلى كل الراغبين في ذلك باستعمال أنجع الوسائل التقنية،

- المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه الخاصة وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون،

- إعطاء مشتركيه معلومات واضحة ودقيقة حول موضوع النفاذ إلى خدمات "انترنات" ومساعدتهم كلما طلبوا ذلك،

- عرض أي مشروع خاص باستعمال منظومات الترميز على اللجنة،

- احترام قواعد حسن السيرة بالامتناع خاصة عن استعمال أية طريقة غير مشروعة سواء اتجاه المستخدمين أو اتجاه مقدمي خدمات "انترنات" الآخرين،

- تحمل مسؤولية محتوى الصفحات وموزعات المعطيات التي يستخرجها ويأويها طبقا للأحكام التشريعية المعمول بها،

- اتخاذ كل الاجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات المفتوحة لمشتركيه قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الأخلاق".

وفي المجال نفسه، وإضافة للالتزامات السابق ذكرها بموجب نص المادة (14)، نصت المادة (11) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على مجموعة أخرى من الالتزامات، حيث تنص على:" مع مراعات طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ:

أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها..."

من جهة أخرى، حدد المشرع مدة حفظ المعطيات بسنة واحدة، وذلك بموجب نص المادة (7/11) من القانون 09-04 التي تنص على: "تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل..."، قصد إعطاء الوقت اللاّزم لأجهزة البحث والتحري للرجوع إلى هذه المعطيات في حال الحاجة إليها.

ونظرا لأهمية هذا الفضاء الافتراضي فلمزودي خدمة الإنترنت مسؤولية كبيرة في الحد من المخاطر التي تعترض شبكة الإنترنت، لذا يجب عليهم اتباع سياسة تأمينية علمية لحماية أنظمة المعلومات من قبل مخترقي الأنظمة مثل: تنظيم عمليات دخول مستخدمي النظام وتأمين الشبكة الداخلية والخارجية وتأمين التطبيقات وقواعد البيانات المستخدمة...إلخ[1].

من جهة ثانية أضاف المشرع الجزائري التزامات أخرى بموجب نص المادة (12) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي تنص على:" زيادة على الالتزامات المنصوص عليها في المادة (11) أعلاه، يتعين على مقدمي خدمات الإنترنت ما يأتي:

أ- التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين، وتخزينها أو جعل الدخول إليها غير ممكن.

ب-وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها" .

وعليه يلعب مزود خدمة الإنترنت دورا فعالا في مساعدة السلطات القضائية المكلفة بالتحريات والتحقيقات في ضبط الدليل الرقمي لإدانة المتهم، إذ يمكن عن طريق برامج متخصصة مثل: برنامج *(Carnivore)* –سبق التطرق إليه–الوصول إلى الفاعل عن طريق تتبع خطواته عبر شبكة الإنترنت كما يقوم بدور وقائي قبل وقوع الجريمة، وذلك من خلال وضع ترتيبات تقنية تسمح بتوفير حراسة دائمة لمضمون الموزعات المفتوحة لمشتركيه، قصد منع النفاذ إلى الموزعات التي تحتوي معلومات تتعارض مع النظام العام أو الأخلاق حماية للمجتمع من الجرائم الإلكترونية.

غير أنه بالرجوع إلى الواقع الفعلي، نلاحظ أن هناك عدم تطبيق لبعض هذه النصوص خاصة ما تعلق بحجب المواقع التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها والتي تؤدي غالبا إلى توفير مناخ ارتكاب الجرائم الإلكترونية خاصة ما

---

[1] عماد مجدي عبد الملك، المرجع السابق، ص40، راجع أيضا، *Christiane Féral Schuhl, art-Cit,p.123.*

تعلق بالشرف والاعتبار، بل يشترط بعض مزودي خدمات الإنترنت شراء برنامج بسعر مكلف لتعطيل النفاذ لهذه المواقع، وهو ما لا يقدر على دفعه جل المشتركين.

من ناحية أخرى أدى انتشار ما يعرف بمقاهي الإنترنت *(Cybercafé)* التي توفر الخلوة والخصوصية لمستعمليها خاصة فئة الشباب والمراهقين بعيدا عن مراقبة الأهل، وبالرغم من أن القانون يلزم مالكي هذه الأماكن بإيقاف وتعطيل المواقع الإباحية والمخلة بالنظام العام، إلا أن بعض مالكي هذه الفضاءات يضربون عرض الحائط هذه القوانين، وما يزيد الطين بلة هو تعمّد هؤلاء التغاضي عن بعض السلوكات اللاّأخلاقية لبعض المراهقين والشباب على اعتبار أنهم من زبائنهم الأوفياء، كما يقوم بعضهم بتجهيز محله بالأضواء الخافتة ووضع الحواجز بين الزبائن لتوفير المزيد من الخصوصية، مما يساعد على انتشار الجرائم الإلكترونية.

ثانيا: مسؤولية مقدمي خدمة الإنترنت: مما سبق ذكره عرفنا أن مقدمي خدمات الإنترنت يقومون بدور فني بحت في توصيل المشترك إلى شبكة الإنترنت، ولا علاقة لهم بالمادة المعلوماتية المنشورة من طرف الزبون. لكن ورغم ذلك ثار جدال فقهي حول مدى مسؤوليتهم الجنائية، وبرز في هذا الشأن ثلاث اتجاهات:

الاتجاه الأول: يرى عدم مسؤولية مزودي الخدمة على الإطلاق لأن دوره فنيّ بحت، حتى ولو كان ضمن مهامه إيواء المعلومات، كما أن مزود الخدمة لا يملك القدرة على التحكم في أي مضمون يبث على الشبكة والقول بتقرير مسئوليته هنا يناظر القول بمساءلة مدير مكتب البريد والهواتف على مدى مشروعية الخطابات والمكالمات التي تجري عبر هذه الخطوط. لكن تبقى مشكلة هذا الرأي في صعوبة قبوله في حالة ما إذا قام مزود الخدمة باقتراح المادة المعلوماتية التي يتم بثها فهو بمثابة متعهد معلومات أو منتج، وبالتالي يُسأل جنائيا عن المادة غير المشروعة التي يبثها للجمهور على الشبكة[1].

الاتجاه الثاني: يرى مساءلة مزود الخدمة على أساس قواعد المسؤولية الجنائية طبقا لأحكام مسؤولية التابع عن أفعال المتبوع، وذلك لأن المشرع أقام نظاما يتعلق بكيفية النشر على الإنترنت ومزود الخدمة حلقة في هذه السلسلة، لذلك فهو ملزم بمحو المعلومات غير المشروعة، كما لا يعتد بعدم علمه بهذه المواد على اعتبار أنه موزع للمادة المعلوماتية. لكن يصعب أيضا قبول هذا الرأي لأن متعهد الخدمة، ما هو إلا مجرد وسيط فني يقتصر دوره على تمكين المشترك من ولوج شبكة الإنترنت أو الخدمة، وبالتالي لا يمكن مساءلته جنائيا[2].

---

[1] عبد الفتاح بيومي حجازي، الجرائم المستحدثة، المرجع السابق، ص95.

[2] جميل عبد الباقي الصغير، الجرائم الناشئة عن استخدام الحاسب الآلي، المرجع السابق، ص119.

الاتجاه الثالث: يرى أنصار هذا الرأي عدم مساءلة متعهد الخدمة مطلقا، لكن يتوقف الأمر على طبيعة الدور الذي يقوم به، لاسيما وأنه يقوم بأدوار متعددة، فقد يكون متعهدا للإيواء أو التخزين، وقد يكون ناقلا للمعلومات أو لمؤتمرات المناقشة في المجموعات الإخبارية أو على صفحات التواصل الاجتماعي عبر شبكة الإنترنت. وعليه ووفقا لهذا الرأي لو كان متعهد الخدمة مجرد ناقل فلا تقوم المسؤولية الجنائية عن مراقبة المادة المعلوماتية التي يتم نقلها، أما إذا كان دوره غير ذلك فيسأل جنائيا[1]. وعليه يسأل مزود الخدمة إذا كان عالما بمحتوى المادة المجرمة المنشورة عبر الخدمة التي يوفرها أو كان هو من طلبها أو قام بتعديلها[2].

بالنسبة للمشرع الجزائري أخذ بالمسؤولية الجنائية لمقدمي خدمة الإنترنت، وذلك ما نستخلصه من نص المادة (14) من المرسوم التنفيذي رقم:98-257 المؤرخ في:1998/08/25 يضبط شروط وكيفيات إقامة خدمات انترنات واستغلالها، مثل: تحمل مسؤولية محتوى الصفحات واتخاذ كل الإجراءات اللازمة لتأمين حراسة دائمة لمضمون الموزعات والمحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه...إلخ. وأيضا بموجب المادتان (12-11) سالفتي الذكر من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك اعتمادا على مبرّرات واقعية مقبولة نظرا لإساءة استخدام هذا الفضاء السبراني بما يخالف النظام العام والآداب العامة ووقاية للمجتمع من خطر الجرائم الإلكترونية.

بالرجوع إلى نص المادة (8/11) من القانون 09-04 سالف الذكر التي تنص على:"... دون الاخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة(6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000دج إلى 500.000دج .

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات".

من جهة أخرى، ألزم المشرع الجزائري مزودي خدمة الإنترنت تحت طائلة العقوبات، كتمان سرية العمليات التي ينجزونها، وذلك وفق نص المادة (2/10) من القانون 09-04 التي تنص على:" ...ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين...".

---

[1] عبد الفتاح بيومي حجازي، الجرائم المستحدثة، المرجع السابق، ص96، راجع أيضا،
Quéméner(Myriam) et Charpenel (Yves),Op.Cit,p.40.

[2] *Quéméner (Myriam) et Ferry (Joel), Op.Cit,pp.55-56, voir aussi, Mohammed Buzubar, art-Cit,pp.55-56.*

من جانب آخر عاقب المشرع على إفشاء الأسرار بمناسبة تأدية المهام بموجب المادتين (301-302) من (ق.ع.ج) .

وأخيرا يمكن القول أن المشرع الجزائري وُفّق إلى حد بعيد في فرض التزامات بالغة الأهمية بالنسبة لمقدمي الخدمات، والهدف من ذلك أولا: حماية حقوق الزبائن وضمان تقديم أحسن الخدمات في هذا الفضاء، وثانيا: تمكين السلطات القضائية المكلفة بالتحريات والتحقيقات الاستفادة من تكنولوجيات الإعلام والاتصال في الكشف عن الجرائم الإلكترونية والوقاية منها ضمانا لعدم افلات المجرم الإلكتروني من العقاب. ويبقى الأمر المهم التأكد من تطبيق هذه الالتزامات على أرض الواقع خاصة في ظل التطور المذهل والسريع لتكنولوجيات الإعلام والاتصال.

لكن بالمقابل هل اكتفى المشرع الجزائري بفرض هذه الالتزامات فقط للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال؟ أم أن هناك إجراءات أخرى نص عليها في القانون 09-04 سالف الذكر؟ هذا ما سنراه في المبحث الثاني والثالث على التوالي.

المبحث الثاني: في مجال تفتيش المنظومة المعلوماتية وحجز المعطيات

تشكل شبكة الإنترنت وسيلة التعامل اليومي في شتى الميادين، غير أن إساءة استخدامها، أفرز أنماطا مستحدثة من الجرائم لم يكن للبشرية سابق عهد بها، فهي معقدة في طرق ارتكابها ووسائل كشفها وتشكل هاجسا أمنيا للأفراد والدول على حد سواء مستغلة في ذلك أحدث التكنولوجيات في مجال تقنيات الكمبيوتر والأنظمة المعلوماتية، وفي هذا الصدد تقول " روى جودسون " خبيرة بمركز المعلومات الوطني الأمريكي "لقد أصبحت الجريمة أكثر قوة بفضل التقنية الحديثة[1]، ما يتطلب ضرورة توفير وسائل وإجراءات حديثة للجهات القضائية المختصة لمحاربة هذه النوع من الجرائم .

وعليه يطرح التساؤل الآتي: ماهي القواعد الإجرائية الخاصة التي أقرها المشرع الجزائري في مجال تفتيش وحجز المنظومات المعلوماتية؟.

سنتناول ماهية التفتيش في (المطلب الأول)، ثم نتطرق إلى تفتيش المنظومة المعلوماتية والجهة القضائية المختصة بذلك في (المطلب الثاني)، ثم نبحث في إجراء تمديد التفتيش إلى منظومة معلوماتية أخرى في (المطلب الثالث)، ونختم في الأخير بإجراء حجز المعطيات المعلوماتية في (المطلب الرابع).

المطلب الأول: ماهية التفتيش

[1] علي عبد القادر القهوجي، المرجع السابق، ص7.

حقّقت الثورة التكنولوجية قفزة هائلة في مجال تقنية المعلومات، بالمقابل أدى سوء استخدامها إلى ظهور جرائم مستحدثة عرفت بالجرائم المعلوماتية، مما صعب من مكافحتها نظرا لطبيعتها وخصوصية إجراءات التحقيق فيها عبر هذه البيئة الافتراضية لتعقّب المجرم المعلوماتي. في هذا الصدد نص القانون رقم: 09-04 المؤرخ في:05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على جملة من القواعد الإجرائية المتعلقة بتفتيش المنظومة المعلوماتية وحجز المعطيات، إذ يعتبر هذا القانون قفزة نوعية في السياسة الجنائية الإجرائية للمشرع بخصوص الإجراءات الجزائية المتعلقة بمكافحة الجريمة ضمن نطاق العالم الافتراضي، منسجما في ذلك مع نصوص (إ.أ.م.إ.م) و(إ.ع.م.ج.ت.م) كما سنوضحه لاحقا. وقبل الحديث عن الإجراءات الخاصة بتفتيش المنظومة المعلوماتية، لا بد أولا من التطرق إلى تعريف التفتيش في (الفرع الأول) ثم نتطرق ثانيا إلى خصوصية التفتيش الواقع على المنظومة المعلوماتية في (الفرع الثاني) .

الفرع الأول: تعريف التفتيش:

يعتبر إجراء التفتيش وفقا للضوابط التقليدية "عملية بحث في مستودع السر عن أدلة الجريمة وكل ما يفيد في كشف الحقيقة"[1]، ففي هذه الحالة لا مشكلة، ولكن يثار التساؤل حينما نكون أمام إجراء التفتيش والحجز في مجال الجرائم المرتكبة على منظومة معلوماتية تخزن بيانات ومعلومات معالجة إلكترونيا. فحينما ينصب التفتيش على الكيان المادي للحاسوب *(Hardware)* وهي الأشياء الملوسة من أجزائه وأدواته التي تعمل بشكل متكامل لأداء مهمة في معالجة البيانات آليا لا مشكلة في ذلك، إذ يمكن ضبطها وحجزها، ولكن تبرز الصعوبة حينما نكون بصدد تفتيش وحجز المكونات المعنوية أو المنطقية للحاسوب *(Software)* كالبرامج وقواعد البيانات...إلخ، والمتمثلة أساسا في برامج النظام الضرورية لتشغيل الحاسوب إضافة إلى برامج التطبيقات التي تهدف إلى حل المشكلات المتعلقة باستعماله. وباعتبار تحول الجريمة الإلكترونية إلى ظاهرة عالمية يصعب معها الكشف عن مرتكبها نظرا لطبيعتها الخاصة، واستخدامها لأحدث تكنولوجيات الكمبيوتر والأنظمة المعلوماتية، مما يتطلب ضرورة توفير وسائل وإجراءات حديثة للجهات القضائية المختصة لمحاربة هذا النوع من الجرائم[2].

من جانب آخر، يعتبر التفتيش من أخطر الحقوق التي مُنحت للمحقق، وذلك لمساسها بالحقوق المكفولة دستوريا، لذا يحيطها المشرع بجملة من الضوابط تكون ضمانا للحرية الفردية أو حرمة

---

[1] علي حسن محمد الطوالبة، التفتيش الجنائي عن نظم الحاسوب والإنترنيت، عالم الكتب الحديث، الأردن، 2004، ص10.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص239.

المسكن[1]، فإذا كانت الجريمة واقعة على المكونات المادية للكمبيوتر فلا عائق يحول دون تطبيق نصوص القواعد التقليدية للتفتيش المنصوص عليها بموجب (ق.إ.ج.ج)[2]، لكن تبرز المشكلة حينما نكون بصدد تفتيش المكونات المنطقية للكمبيوتر وبياناته، فبإمكان الجاني التخلص من البيانات التي يستهدفها التفتيش عبر إتلافها أو إرسالها من خلال نظام معلوماتي إلى نظام معلوماتي آخر، ناهيك عن عدم إجبار الجاني الكشف عن الكلمة السرية *(pass Word)* بغرض الدخول لهذه البيانات وتفتيشها[3]، إذ تعبر جرائم نظم المعلومات على السلوك السيئ المتعمد الذي يستخدم نظم المعلومات لإتلاف المعلومات أو إساءة استخدامها [4].

من جهة أخرى، لم يضع المشرع الجزائري تعريفا للتفتيش شأنه في ذلك شأن جل التشريعات المقارنة ، فقد اعتبره إجراء من إجراءات التحقيق الهدف منه الحصول على الأدلة لإثبات الجريمة وبالتالي الوصول للجاني، لذا أحاطه بجملة من الضوابط الصارمة لما يترتب عنه من مساس بحرية الأشخاص وكرامتهم وحرمة ممتلكاتهم[5]. في هذا الشأن نصت المادة (47) من التعديل الدستوري المؤرخ في:2016/03/06 على:" تضمن الدولة عدم انتهاك حرمة المسكن، فلا تفتيش إلا بمقتضى القانون، وفي إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة ".كما نص عليه المشرع في المواد من:(44-47) والمادة (64) إضافة إلى المادة (79) وما بعدها من (ق.إ.ج.ج).

ونظرا لخطورة هذا الإجراء، تكفل كل من الفقه والقضاء بمحاولة إعطاء تعريفات للتفتيش منها أنه:" إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون، يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه" [6]،أو هو: " تفتيش شخص المتهم للبحث معه في مستودع سره عن أشياء تفيد في الكشف عن الجريمة ونسبتها إلى المتهم"[7]. كما عرّفه أخرون أنه:" الاطلاع على محل له حرمة للبحث عما يفيد

---

1 خالد ممدوح ابراهيم، فن التحقيق، المرجع السابق، ص180.

2 المواد (45) و (47) و (79) و ما بعدها من (ق.إ.ج.ج).

3 خالد ممدوح ابراهيم، فن التحقيق، المرجع السابق، ص187.

4 حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف للعلوم الأمنية، الرياض، السعودية، ط1، 2000، ص23.

5 زيدان زيبحة، المرجع السابق، ص130.

6 منى جاسم الكواري، التفتيش، شروطه وحالات بطلانه- دراسة مقارنة، منشورات الحلبي الحقوقية بيروت، ط1، 2008، ص23.

7 أحمد عبد الحكيم عثمان، تفتيش الأشخاص وحالات بطلانه من الناحيتين العلمية والعملية، منشأة المعارف، الإسكندرية مصر،2002، ص13.

التحقيق"[1] أو هو:" البحث عن شيء يتصل بجريمة وقعت وتفيد في كشف الحقيقة عنها وعن مرتكبيها، وقد يقتضي التفتيش في محل له حرمة خاصة"[2].

من جانب آخر ينطوي التفتيش على خصائص ثلاثة[3] تجعل منه إجراء ضروريا هدفه ضبط الأدلة تمهيدا للوصل إلى مرتكب الجريمة وتقديمه للعدالة وممارسة حق المجتمع عليه في العقاب.

الفرع الثاني: خصوصية التفتيش الواقع على المنظومة المعلوماتية:

قد يتطلب التحقيق تفتيش شخص المتهم أو منزله قصد ضبط الأشياء المحصلة من الجريمة وبالتالي فإجراء التفتيش هو أصلا من اختصاص سلطة التحقيق واستثناء النيابة العامة[4]، فحينما ينصب التفتيش على الكيان المادي للحاسوب لا مشكلة في ذلك، إذ أنه يمكن ضبط مكونات الحاسوب المختلفة و حجزها، ولكن يثار التساؤل حينما نكون بصدد تفتيش المكونات المعنوية أو المنطقية للحاسوب كالبرامج وقواعد البيانات...إلخ. حيث عرف المجلس الأوروبي هذا النوع من التفتيش بأنه:" إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني"[5].

وقبل أن نفهم إجراءات وقواعد التفتيش في مجال المنظومة المعلوماتية ، لا بد من التطرق إلى معنى المكونات المادية والمعنوية للحاسوب:

أولا: المكونات المادية للحاسوب *(Hardware)*: يقصد بالمكونات المادية للحاسوب بأنها:" الأشياء الملوسة من أجزائه وأدواته التي تعمل بشكل متكامل لأداء مهمة في معالجة البيانات آليا"[6] وعليه يتكون الحاسوب عموما من وحدات ثلاث هي: وحدات الإدخال ووحدات المعالجة ووحدات الإخراج، فمثلا: تتمثل وحدات الإدخال في لوحة المفاتيح وشاشات اللّمس ونظام الإدخال المرئي والصوتي، إضافة إلى وحدة الذاكرة الرئيسية التي تستخدم في الحفظ الدائم أو المؤقت للبيانات والمعلومات والبرامج، كما تتمثل أيضا وحدات المعالجة في وحدة التحكم أو وحدة المعالجة المركزية التي تقوم بمعالجة البيانات والتنسيق بين الوحدات الأخرى وضبط التعليمات...إلخ. وأخيرا وحدات

---

[1] سليم علي عبده، التفتيش في ضوء قانون أصول المحاكمات الجزائية الجديد–دراسة مقارنة، منشورات زين الحقوقية، بيروت، لبنان ط1، 2006، ص25.

[2] فؤاد حسين العزيزي، المرجع السابق، ص196.

[3] ينطوي التفتيش على خصائص ثلاثة هي: الجبر أو الإكراه، والمساس بحق السر، والبحث عن الأدلة المادية للجريمة، لأكثر تفاصيل راجع، سليم علي عبده، المرجع السابق، ص ص 31–33، وأيضا، سامي جلال فقي حسين، التفتيش، المرجع السابق، ص57 وما بعدها.

[4] نبيلة هبة هروال، المرجع السابق، ص221.

[5] علي عدنان الفيل، إجراءات التحري، المرجع السابق، ص39.

[6] بلال أمين زين الدين، المرجع السابق، ص22.

الإخراج وتسمى أيضا بوسائط إظهار نتائج التشغيل ومعالجة البيانات كالشاشة والطابعة والراسم والأقراص المرنة والصلبة التي تعتبر من أشهر تخزين البيانات والمحافظة عليها[1].

وعليه ليس هناك خلاف في أن الدخول إلى المكونات المادية للحاسوب بحثا عن دليل ما يوصلنا إلى مرتكب الجريمة الإلكترونية، يخضع للإجراءات التقليدية للتفتيش، أي طبيعة المكان الموجودة فيه تلك المكونات، وهل هو من الأماكن العامة أو الخاصة، فمثلا: إذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكن المتهم باتباع الإجراءات والضمانات المكفولة قانونا كحضوره شخصيا أو من ينوب عنه[2].

ثانيا: المكونات المعنوية(المنطقية) للحاسوب *(Software)*: يُطلق أيضا على المكونات المعنوية للحاسوب بالبرمجيات، وهي عبارة عن برامج معينة تخزن أو توضع في وسائل تخزين خاصة كي يمكن استخدامها من قبل الكمبيوتر نفسه، فهي عبارة عن شفرات خاصة لذا سُميت بالكيان المنطقي، كما تعتبر بمثابة العمود الفقري وعصب عمل الكمبيوتر، إذ توفر إمكانات وسرعة فائقة في إنجاز المهام المطلوبة[3]، كما يُعرف الكيان المنطقي للحاسوب لغة، بأنه كلمة تستخدم للدلالة على جميع المكونات غير المادية لنظام الحاسوب كبرامج النظام الضرورية لتشغيل الحاسوب إضافة إلى برامج التطبيقات التي تهدف إلى حل المشكلات المتعلقة باستعمال الحاسوب. من جهة أخرى، عرفه القانون الأمريكي الصادر سنة 1980 بأنه: " مجموعة توجيهات أو تعليمات يمكن للحاسب استخدامها بشكل مباشر أو غير مباشر للوصول إلى نتيجة معينة"[4].

---

[1] يتكون الكمبيوتر من مجموعة من المعدات والأجهزة يمكن تقسيمها إلى أربعة مجموعات هي :

– وحدة المعالجة المركزية: *(Processing Unit Central)*: من مهامها معالجة البيانات والمعطيات المدخلة للحاسوب...إلخ.

– وحدات إدخال *(Input Units)*: تختص بمهمة إدخال التعليمات والأوامر والبيانات للحاسوب باستعمال طرق مختلفة كلوحة المفاتيح...إلخ.

– وحدات إخراج *(Units Output)*: بعد تنفيذ التعليمات ومعالجة البيانات، تخرج في شكل مرئي على الشاشة أو ورقي باستعمال الطابعة...إلخ.

– وحدات تخزين*(Storage Units)*: مهمتها تخزين البرامج والبيانات المعالجة، كما تقسّم إلى وحدات تخزين داخلية كالقرص الصلب ووحدات تخزين خارجية كالأقراص المرنة والمضغوطة والذاكرة الوميضية...إلخ، راجع، طارق إبراهيم الدسوقي عطية، المرجع السابق، ص ص 88 – 95.

[2] خالد ممدوح إبراهيم، فن التحقيق، المرجع السابق، ص195.

[3] بلال أمين زين الدين، المرجع السابق، ص23.

[4] طارق إبراهيم الدسوقي عطية ، المرجع السابق، ص99.

وفي الاتجاه نفسه، عرّف التوجيه الأوروبي الصادر في: 14 ماي 1991 برامج الحاسب الآلي بأنها:" مجموعة من الأوامر التي تؤدي إلى إنجاز المهام المستهدفة من خلال نظام معالجة المعلومات والذي يطلق عليه اسم الحاسب"[1]، كما يمكن تقسيم برامج الحاسوب إلى نوعين: الأول: برامج النظام *(System Programs)* والذي دونه لا يمكن استغلال الحاسوب، ويتضمن نظم التشغيل والبرامج المساعدة ونظام إدارة قواعد البيانات...إلخ، والثاني: برامج التطبيقات أو الكيانات المنطقية التطبيقية *(Application Programs)* ، والتي تقوم بمهام محددة، مثل: برامج معالجة النصوص، أو برامج توجه لخدمة وظيفة معينة كبرامج إدارة الموارد البشرية...إلخ[2].

مما سبق ذكره يعتبر إجراء التفتيش على المكونات المنطقية للحاسوب من الصعوبة بمكان نظرا للطبيعة المعنوية الخاصة لهذه المعطيات المخزنة إلكترونيا سواء كان ذلك على مستوى حاسوب واحد أم كان مرتبطا بحواسيب أخرى ضمن الشبكة العنكبوتية، إذ يتطلب ذلك مثلا الكشف عن الرقم السري أو الكود*(Code)*،أو كلمة السر*(Password)*[3] أو نظام التشفير أو ترميز البيانات للولوج إلى مختلف الملفات، ومن ثمة الاطلاع عليها وتقديمها كدليل إلكتروني يدين المتهم[4].

المطلب الثاني: تفتيش المنظومة المعلوماتية والجهة المختصة بذلك

تكمن وظيفة نظم المعلومات في معالجة وتجميع واسترجاع وتخزين ونشر المعلومات سواء داخل منظومة معلوماتية واحدة أو متصلة بمنظومة معلوماتية أخرى، وسواء داخل الإقليم الوطني أو خارجه ، سنتطرق إلى تفتيش المنظومة المعلوماتية في (الفرع الأول)، ثم نتعرف على الجهة القضائية المختصة بذلك في (الفرع الثاني).

الفرع الأول: تفتيش المنظومة المعلوماتية:

إن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، تطلب تدخلا تشريعيا صريحا سواء على المستوى الدولي أو الداخلي، حيث يهدف التفتيش الدخول إلى المنظومة المعلوماتية وملحقاتها والتي تحتوي على بيانات مخزنة يمكن أن تشكل دليلا رقميا لإدانة المتهم[5]. ففي إطار تفتيش المنظومة المعلوماتية، نصت المادة (1/19) من (إ.أ.م.إ.م) على:

---

1 خالد ممدوح إبراهيم، أمن الجريمة، المرجع السابق، ص66.

2 طارق إبراهيم الدسوقي عطية، المرجع السابق، ص100.

3 كلمة السر: كلمة يحتفظ بها مستخدم الحاسب سرا ويطلبها الحاسب منه قبل التعامل للتأكد من شخصية المستخدم، نبيلة هبة هروال المرجع السابق، ص 355.

4 عادل عزام سقف الحيط، المرجع السابق، ص ص239-240.

5 *Quéméner(Myriam) et Charpenel (Yves),Op.Cit,p.177 .*

" 1–على كل دولة طرف أن تعتمد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لتمكين السلطات المختصة من الدخول والتفتيش إلى:

أ– إلى منظومة معلوماتية أو جزء منها والبيانات المخزنة فيها.

ب– إلى وسائط تخزين البيانات الموجودة على إقليمها..."[1].

وفي الشأن ذاته، نصت أيضا المادة (1/26) من (إ.ع.م.ج.ت.م) تحت عنوان:" تفتيش المعلومات المخزنة" على:

"1– تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى:

أ– تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها،

ب–بيئة أو وسيط تخزين معلومات تقنية معلومات تقنية معلومات والذي قد تكون معلومات مخزنة فيه أو عليه...". وعليه أجازت الاتفاقيتان تفتيش المنظومة المعلوماتية عن طريق الدخول بغرض التفتيش ولو عن بعد إلى المنطومة المعلوماتية أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها، ووسائط تخزين البيانات الموجودة على إقليمها، نظرا لما يمثله هذا الإجراء من أهمية في الحصول على الدليل الرقمي لإدانة المتهم.

من جانب آخر، كلفت اللجنة الأوروبية في إطار تطبيق(إ.أم.إ.م) فريق بحث قصد وضع برمجيات تسمح بإجراء تفتيش وحجز المعطيات في القوت الفعلي *(online)* من أجل استخلاص الأدلة الرقمية قبل تقديمها أمام القاضي، تسمى هذه التقنية بـ" البحث عن الدليل الرقمي على المباشر"(*cybertools online search evidence*)[2].

كما قام المشرع الجزائري للسبب نفسه بتعديل قانون العقوبات بإضافة قسم سابع مكرر عنوانه: "المساس بأنظمة المعالجة الآلية للمعطيات"[3]، حيث كان الهدف هو حماية نظام المعالجة الآلية

[1] ***Article 19 – Perquisition et saisie de données informatiques stockées***

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a. à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b. à un support du stockage informatique permettant de stocker des données informatiques sur son territoire..., convention européenne de la cybercriminalité, Op.Cit,p.10.

[2] *Christiane Féral Schuhl, art-Cit,p.115.*

[3] آمال قارة، المرجع السابق، ص100.

للمعطيات كما سنرى لاحقا، ونظام المعالجة الآلية للمعطيات تعبير فني تقني حديث يخضع للتطورات المتلاحقة في مجال صناعة الكمبيوتر وملحقاته وبرامجه. في هذا الصدد عرّفت المادة (2/02) من القانون رقم 09-04 مؤرخ في:05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المنظومة المعلوماتية: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، مترجما بذلك نص المادة (01/أ) من (إ.أ.م.إ.م)، ومتوافقا أيضا مع نص المادة (5/02) من (إ.ع.م.ج.ت.م) التي عرفت النظام المعلوماتي على أنه:" مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات".

وفي تعريف آخر بأنها: "مجموعة من الإجراءات التي يتم من خلالها تجميع واسترجاع أو تشغيل وتخزين ونشر المعلومات بغرض دعم عمليات صنع القرار وتحقيق الرقابة داخل الجهة الإدارية أو أيا كانت شكل تلك المنظمة"[1]، كما عُرف أيضا النظام المعلوماتي على أنه:" جهاز يتكون من مكونات مادية ومكونات منطقية وذلك بغرض المعالجة الآلية للبيانات الرقمية، وهو يشتمل على وسائل الإدخال والإخراج وتخزين البيانات[2]، وهذا الجهاز قد يكون منفردا أو متصلا بمجموعة من الأجهزة المماثلة عن طريق شبكة"[3].

وعليه تقوم المنظومة المعلوماتية على وجود نظام تشغيل حاسوبي سواء كان منفصلا أو متصلا سلكيا أو لا سلكيا يقوم واحد منها بالمعالجة الآلية للمعطيات تنفيذا لبرنامج معين، حيث نجد أن التعريفات المختلفة لنظم المعلوماتية تطابقت مع تعريف المشرع الجزائري مما يمكن من تحديد أدق للعناصر المكونة للجريمة الواقعة على الأنظمة المعلوماتية، رغم الصعوبات التي يصادفها رجال الضبطية القضائية والمحققين في تفتيش وضبط الجرائم الإلكترونية بسبب طبيعتها الخاصة، فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود[4].

غير أن المشرع خرج عن هذا المبدأ واستبق الأحداث، حيث جعل من إجراء التفتيش مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة الإلكترونية، وذلك من خلال القيام بعمليات المراقبة المسبقة وفق نص المادة (03) من القانون رقم: 09-04 السالف الذكر التي تنص على:" مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو

[1] أيمن عبد الله فكري، جرائم نظم المعلومات-دراسة مقارنة، رسالة دكتوراه، جامعة المنصورة، مصر ، 2006، ص11.

[2] عرفت المادة (3/02) من (إ.ع.م.ج.ت.م) مصطلح البيانات: "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات كالأرقام والرموز والحروف..."

[3] نبيلة هبة هروال، المرجع السابق، ص335.

[4] يوسف المصري، المرجع السابق، ص217.

لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية" .

في الصدد نفسه، نصت المادة (2/04) من القانون نفسه على :"في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني"[1]، وهو الهدف نفسه الذي أكدته المادة (01) من القانون نفسه التي تنص على:" يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها".

من جهة أخرى، يهدف التفتيش المنصبّ على المنظومة المعلوماتية إلى استخلاص الدليل الإلكتروني، قبل قيام المجرم المعلوماتي بتدميره أو إخفائه للإفلات من العقوبة، وعليه أدرج المشرع الجزائري إجراء التفتيش في مجال الجرائم الإلكترونية في قانون الإجراءات الجزائية، استجابة لنصوص كل من (إ.أ.م.إ.م) و(إ.ع.م.ج.ت.م)، حيث يختلف التفتيش في هذه الحالة عن التفتيش العادي، فهو يتوقف أساسا على طبيعة المكان الذي يحتوي على أجهزة الكمبيوتر ومكوناته، وفيما إذا كان خاصا أم عاما ناهيك عن تحديد الإقليم إذا كان وطنيا أم أجنبيا[2]، فلقد نصت المادة(05) من القانون رقم: 09-04 تحت عنوان: "تفتيش المنظومات المعلوماتية" على:" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه، الدخول بغرض التفتيش ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية..."

فمن خلال هذه المادة أجاز المشرع الدخول بغرض التفتيش ولو عن بعد إلى المنظومة المعلوماتية ودون إذن صاحبها، وهذا برغم تمتع برامج الحاسوب وقواعد البيانات بالحماية القانونية بموجب القانون رقم: 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، والذي تناولناه سابقا. ونظرا لصعوبة تنفيذ هذا الإجراء من الجانب التقني، أجاز المشرع بموجب المادة (6/05) من القانون رقم:09-04 سالف الذكر الاستعانة بكل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية، وهذا ما أكدت عليه أيضا المادة (4/19) (إ.أ.م.إ.م)

---

[1] المادة (04) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] زيدان زيبحة، المرجع السابق، ص133.

فيما يخص الاستعانة بكل شخص له دراية بعمل المنظومة المعلوماتية أو بإجراءات حماية المعطيات المعلوماتية[1]، والأمر ذاته أكدته نص المادة (2/27) من (إ.ع.م.ج.ت.م).

من خلال ما سبق ذكره، يتبين لنا بوضوح أن التفتيش إذا تعلق بالمكونات المادية للحاسوب لا مشكلة في ذلك، ويتم وفقا لأحكام المادة (44) من (ق.إ.ج.ج)، إذ يتطلب إذنا مكتوبا من طرف وكيل الجمهورية أو قاضي التحقيق يُستظهر عند دخول المنزل، كما يتضمن الإذن وصف الجريمة موضوع البحث عن الدليل وحضور الشخص المعني، وعليه يجب الانتقال إلى مكان تواجد جهاز الحاسوب أو أحد مكوناته المادية مثل: الأقراص الصلبة والمرنة والأقراص المضغوطة...إلخ، فمن السهولة هنا ضبط جهاز الحاسوب ومكوناته وملحقاته وحجزها وتقديمها كدليل لإدانة المتهم، لكننا هنا بصدد التفتيش الذي يستهدف الكيان المنطقي للحاسوب، وسواء استهدف المنظومة المعلوماتية كلها أو جزء منها، أو منظومة تخزين معلوماتية[2]، فالتفتيش في كلتا الحالتين يستهدف في مفهومه أشياء غير مادية.

ونظرا لما تتطلبه العملية من جانب تقني معقد، أجاز المشرع الجزائري نسخ وإفراغ المعطيات على دعامة تخزين إلكترونية تكون قابلة للحجز، مثل: الأقراص المرنة والأقراص المضغوطة والذاكرة الومضية...إلخ، وهذا بموجب نص المادة (06) من القانون رقم: 09-04 :"عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة...يتم نسخ المعطيات محل البحث وكذا المعطيات اللاّزمة لفهما على دعامة تخزين الكترونية...". كما ينبغي أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية سواء بوصفه فاعلا أو شريكا[3].

لكن ما هي الجهة القضائية المختصة بمنح الإذن بالتفتيش؟ هذا ما سنتناوله في الفرع الموالي.

الفرع الثاني: الجهة القضائية المختصة بذلك:

[1] ***Article 19 – Perquisition et saisie de données informatiques stockées***

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2, convention européenne de la cybercriminalité, Op.Cit,p.10.

[2] يقصد بمنظومة تخزين معلوماتية: المنظومة التي تحتوي على بيانات تأخذ شكلا إلكترونيا أو أي شكل آخر يسمح بمعالجتها مباشرة نبيلة هبة هروال، المرجع السابق، ص 355.

[3] الشحات إبراهيم محمد منصور، المرجع السابق، ص197، راجع أيضا، فؤاد حسين العزيزي، المرجع السابق، ص198.

بالرجوع إلى المادة (04/أ) من القانون رقم: 09-04 السالف الذكر التي تبين كيفيات المراقبة للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، يبين لنا المشرع الجهة القضائية المختصة بهذه الحالة في المادة نفسها الفقرة الأخيرة، إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المنصوص عليها بموجب المادة (13) من القانون نفسه، إذنا لمدة ستة أشهر قابلة للتجديد، وذلك على أساس طبيعة ونوعية الترتيبات التقنية المراد أخذها بخصوص الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية[1].

فيما عدا هذه الحالة الخاصة، وبموجب نص المادة (05) من القانون 09-04 التي تنص على:" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة (04) أعلاه الدخول بغرض التفتيش..." إذ يتعين الرجوع إلى التدابير التي نص عليها (ق.إ.ج.ج) في مجال التحري والتفتيش بالنسبة للجرائم الإلكترونية سواء بالنسبة لوكيل الجمهورية بموجب المادة (37)أو قاضي التحقيق بموجب المادة (40) والذين ينصان على تمديد الاختصاص لكل من وكيل الجمهورية وقاضي التحقيق في جرائم محددة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[2].

وعليه يمكن القول: بأن المشرع الجزائري حدّد بوضوح الجهة المختصة سواء في مجال الإذن بوضع ترتيبات للمراقبة الإلكترونية للحيلولة دون الاعتداء على منظومة معلوماتية، أو في مجال الدخول بغرض التفتيش ولو عن بعد لمنظومة معلوماتية أو جزء منها أو منظومة تخزين معلوماتية سواء تقع داخل الاقليم الوطني أو خارجه كما سنرى لاحقا.

المطلب الثالث: تمديد التفتيش

تمكّن تكنولوجيا المعلوماتية من برمجة وإنشاء منظومة معلوماتية في أي مجال تكون مستقلة بحد ذاتها على نفس جهاز الحاسوب أو متصلة سلكيا أو لا سلكيا بمنظومة معلوماتية أخرى متواجدة في جهاز حاسوب آخر بواسطة الشبكة العنكبوتية العالمية التي تعني لغويا:" الترابط الذي يتم بين الشبكات حيث تتكون من عدد كبير من شبكات الحاسب الآلي المتناثرة في أنحاء كثيرة من العالم"

---

[1] المادة (04) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] المادتان (37) و(40) من (ق.إ.ج.ج).

واصطلاحا تعني: "الوسيلة أو الأداة التواصلية بين الشبكات المعلوماتية دون ما اعتبار للحدود الوطنية"[1]، وهذا يشكل مكانا خصبا للجرائم الإلكترونية مما يصعب من اكتشاف الجريمة وملاحقة مرتكبها، لذا نص المشرع على ضرورة تمديد التفتيش داخل الاقليم الوطني في حالة وجود معطيات مبحوث عنها ومخزنة في منظومة معلوماتية أخرى يمكن الولوج إليها انطلاقا من المنظومة المعلوماتية الأولى (الفرع الأول)، ثم نتطرق إلى تمديد التفتيش خارج الإقليم الوطني في (الفرع الثاني).

الفرع الأول: تمديد التفتيش داخل الاقليم الوطني:

تحسبا لما يقدم عليه المجرم المعلوماتي من ارتكاب جرائم عديدة باستخدام منظومات معلوماتية مترابطة، نص المشرع على تمديد إجراء التفتيش سواء داخل الاقليم الوطني أو خارجه إذا لزم الأمر وذلك بمساعدة السلطات الأجنبية المختصة لكن وفق شروط معينة. حيث تقوم تقنية شبكة الإنترنت على ترابط ملايين أجهزة الحاسوب في العالم، إذ يوفر هذا الفضاء السبراني*(Cyberspace)* خدمات متنوعة في مجالات عديدة، كما توفر هذه التقنية العالية للمجرم الإلكتروني الدخول والانتقال من منظومة معلوماتية لأخرى، بما يمكن معه محو أو تعديل أو تغيير المعطيات ناهيك عن صعوبة تتبعه وايجاد دليل ضده، لذا نص المشرع في المادة (05) من القانون رقم:09-04 علـى:" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة (04) أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطات القضائية المختصة مسبقا بذلك ...". وهو ذاته ما نصت عليه المادة (2/19) من (إ.أ.م.إ.م) على كل طرف أن تعتمد تدابير تشريعية وتدابير أخرى قد تكون ضرورية لسلطات البحث والتحري، للوصول بطريقة سهلة لمنظومة معلوماتية أو جزء منها، عملا بالفقرة (1-أ) ويكون لديهم سبب للاعتقاد بأن البيانات يتم تخزينها في منظومة معلوماتية أو جزء منها وموجودة على إقليمها وهذه البيانات يمكن الوصول إليها بشكل قانوني من خلال المنظومة المعلوماتية الأساسية أو من

---

[1] حسين بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص15.

خلال منظومة معلوماتية أخرى، يجب على السلطات المختصة وعلى وجه السرعة تمديد التفتيش إلى تلك المنظومة..."[1]. والأمر نفسه نصت عليه المادة (2/26) من (إ.ع.م.ج.ت.م).

إن تمديد التفتيش إلى منظومة معلوماتية أخرى مشكوك فيها نظرا لاحتوائها على معلومات مبحوث عنها، يتطلب إجراءات خاصة فهو يتم عن بعد وبشكل سريع، تماشيا مع السرعة الهائلة في نقل المعلومات، وأيضا متى توفر الشك في وجود معطيات مبحوث عنها مخزنة في منظومة معلوماتية أخرى ولكن يتم الوصول إليها عن طريق الدخول من منظومة معلوماتية أولى.

كما نؤكد أن هذه الإجراءات تكتسي طابع الرسمية ولا تتم إلا بعد إعلام الجهات القضائية المختصة تطبيقا لنص المادتين (37) و(40) من (ق.إ.ج.ج) لأنها تندرج ضمن حماية الحياة الخاصة للأفراد المكفولة دستوريا. وبذلك حاول المشرع غلق منافذ إفلات المجرم في هذا النوع المستحدث من الجرائم الذي يتسم بالتعقيد والتطور الدائم في استخدام تقنية المعلومات، مما أجاز معه للسلطات المكلفة بالتفتيش تسخير كل شخص مختص في مجال عمل المنظومة المعلوماتية قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهامها، وهذا وفقا لنص المادة (6/05) من القانون 09-04 السالف الذكر.

الفرع الثاني: تمديد التفتيش خارج الإقليم الوطني:

توفر شبكة الإنترنت الإبحار في عالم افتراضي تتلاشى معه الحدود الجغرافية للدول، مما يخلق صعوبات بالغة لأجهزة البحث والتحري في ملاحقة المجرم الإلكتروني، فقد يتوزع ارتكاب الركن المادي للجريمة الإلكترونية على أكثر من شخص موجودين في أكثر من دولة، مما تنتج عنه مشكلة

---

[1] ***Article 19 – Perquisition et saisie de données informatiques stockées***

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 (a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou un d'un accès d'une façon similaire à l'autre système ..., convention européenne de la cybercriminalité, Op.Cit,p.10.

تنازع الاختصاص بين الدول، لذا عمدت هذه الدول إلى التعاون القضائي وتبادل المساعدة القضائية الدولية فيما بينها بهدف تسهيل إجراءات مكافحة هذا النوع المستحدث من الجرائم.

في هذا الشأن صدرت عن المجلس الأوروبي توصيات، تجيز أن يمتد تفتيش الحاسوب إلى الشبكة المتصل بها ولو كانت تلك الشبكة تقع خارج إقليم الدولة، وذلك بموجب التوصية رقم:13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات على أنه:" لسلطة التفتيش عند تنفيذ تفتيش المعلومات وفقا لضوابط معينة أن تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة، مادامت مرتبطة بشبكة واحدة وأن تضبط البيانات المتواجدة فيها ما دام أنه من الضروري التدخل الفوري للقيام بذلك"[1].

وعلى المسار نفسه، وبعدما نص المشرع الجزائري على تمديد التفتيش داخل الإقليم الوطني اتجه إلى تمديد تفتيش المنظومة المعلوماتية خارج الإقليم الوطني، على اعتبار أن الجرائم الإلكترونية جرائم عابرة للحدود الجغرافية، وبذلك أقر المشرع إجراءات صارمة لملاحقة هذا النوع من الجرائم خارج الإقليم الوطني، وذلك حينما وسّع من نطاق التفتيش بموجب نص المادة (5/05) من القانون رقم:09-04 التي تنص على:" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة (04) أعلاه الدخول بغرض التفتيش ولو عن بعد إلى...إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل...".

وعليه إذا تبيّن لجهات التحقيق أن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزّنة في منظومة معلوماتية تقع خارج الإقليم الوطني، يمكن تتبعها والوصول إليها ولكن ضمن المساعدة الأجنبية التي تتم في إطار الاتفاقيات الدولية ووفقا لمبدأ المعاملة بالمثل لذلك نص المشرع على شروط وقيود المساعدة القضائية الدولية في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، والتي سنتطرق إليها في المبحث الثالث. وهو ما ينسحب أيضا على اختصاص المحاكم الجزائرية بخصوص الجرائم الإلكترونية التي تقع خارج الإقليم الوطني، والتي تضر بمصالح الوطن مثل: استهداف مؤسسات الدولة أو الدفاع الوطني أو سلامة الاقتصاد الوطني، وهذا وفقا لنص المادة (15) من القانون 09-04 التي تنص على:" زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص

---

[1] طارق فوزي الفقي، الرسالة السابقة، ص105.

المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الاقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني".

المطلب الرابع: حجز المعطيات المعلوماتية

يظل الهدف الأساس لعملية تفتيش المنظومة المعلوماتية، هو وضع اليد على الأدلة الرقمية لإدانة المجرم الإلكتروني، فإذا كان حجز الأشياء المادية كالمعدات(المكونات المادية للحاسوب) والأوراق والمستندات...إلخ، لا يعد مشكلة ويتم وفق القواعد الإجرائية التقليدية. غير أن الأمر يختلف تماما، إذ ليس من السهل توقيع الحجز على المنظومة المعلوماتية التي هي في الأصل شيء معنوي غير ملموس.

وعليه يمكن طرح التساؤل الآتي: هل أقر المشرع الجزائري تدابير خاصة لتوقيع الحجز على المنظومة المعلوماتية؟. هذا ما سنجيب عنه في (الفرع الأول). غير أنه من الناحية الواقعية ونظرا للطبيعة الخاصة للأدلة الرقمية، يصعب أحيانا حجز المعطيات المعلوماتية لأسباب تقنية أجاز المشرع للسلطات المختصة القيام بالإجراءات اللاّزمة لمنع الوصول إليها موضحا أيضا حدود استعمال هذه المعطيات(الفرع الثاني).

الفرع الأول: تدابير الحجز:

يقصد بالحجز في قانون الإجراءات الجزائية:" وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها"[1]. يمكن تخزين المعطيات في ذاكرة الحاسوب أو في برامجه إذ تعتبر كيانات غير مادية مما شكل اختلافا في التشريعات العالمية حول مدى اعتبارها قابلة للحجز فلقد نص التشريع الألماني في المادة (94) من قانون الإجراءات الجنائية على أن البيانات المعالجة إلكترونيا لا يسوغ ضبطها إلا بعد تحويلها إلى كيان مادي كنقلها على دعامة إلكترونية، في حين ذهب اتجاه آخر في فرنسا إلى اعتبار برامج الحاسوب كيانا ماديا ملموسا فهو عبارة عن نبضات أو إشارات إلكترونية ممغنطة[2]، في حين أضفى المشرع الجزائري حماية قانونية لقواعد البيانات بموجب نص المادة (05) من الأمر رقم: 03-05 المؤرخ في200/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة التي تنص على:" تعتبر أيضا مصنفات محمية الأعمال الآتية:

---

1 هشام محمد فريد رستم، الجوانب الإجرائية، المرجع السابق، ص93.

2 المرجع نفسه، ص596.

- أعمال الترجمة والاقتباس، والتوزيعات الموسيقية، والمراجعات التحريرية، وباقي التحويرات الأصلية للمصنفات الأدبية والفنية،

- المجموعات والمختارات من المصنفات، مجموعات من مصنفات التراث الثقافي التقليدي وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى، والتي تأتي أصالتها من انتقاء مواد أو ترتيبها...".

وطبقا لنص المادة (06) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تنص على: "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ كل المعطيات اللاّزمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية. يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي يجري بها العملية. غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات".

وهو نفسه ما ذهبت إليه المادة (27) من (إ.ع.م.ج.ت.م) تحت عنوان:" ضبط المعلومات المخزنة" التي تنص على:" تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة(1) من المادة السادسة والعشرين من هذه الاتفاقية، هذه الإجراءات تشمل صلاحيات:

أ- ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات.

ب- عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها،

ج-الحفاظ على سلامة تقنية المعلومات المخزنة.

د-إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها...".

من جانب آخر نصت المادة (3/19) من (إ.أ.م.إ.م) تحت عنوان:" تفتيش وحجز المعطيات المعلوماتية المخزنة" على حجز المنظومة المعلوماتية أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات، إضافة إلى عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها، والحفاظ على سلامة تقنية المعلومات المخزنة...إلخ[1].

---

[1] ***Article 19 – Perquisition et saisie de données informatiques stockées***

والملاحظ أن المشرع الجزائري استعمل مصطلح دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز مثل: القرص المرن والقرص الصلب والقرص المضغوط والذاكرة الوميضية والأشرطة المغناطيسية...إلخ، وترك المجال مفتوحا أمام ظهور تقنيات تخزين جديدة، إذ أنه لا يمكن التعامل مع تلك المعطيات في شكلها الأولى المعنوي وهي عبارة عن نبضات أو ذبذبات الكترونية أو إشارة ممغنطة [1] إلا بعد نسخها على هذه الدعامات كما تتم عملية الحجز وفقا للقواعد المقررة في نص المادة (84) من (ق.إ.ج.ج) كالاطلاع على المستندات المبحوث عنها والاحترام التام لمقتضيات التحقيق وخاصة احترام سر المهنة وحقوق الدفاع بما يكفل أمن وسرية وسلامة المعطيات في المنظومة المعلوماتية وفقا لنص المادة (2/06) من القانون رقم: 09-04.

من ناحية ثانية حرص المشرع الجزائري على سلامة المعطيات المحجوزة من أي حذف أو تغيير بما لا يضر بالدليل الرقمي، وأيضا إعادة تشكيل هذه المعطيات بما يخدم التحقيق بشرط عدم المساس بمحتواها وفقا لنص المادة(3/06) من القانون نفسه، وهذا تحت طائلة العقوبات وفقا لنص المادة (85) من (ق.إ.ج.ج) و هو نفس ما نصت عليه المادتان (07) و (09) من القانون رقم: 09-04 كما سنرى لاحقا. إضافة إلى إجراء الحجز، نص (ق.ع.ج) في المادة(394مكرر06) على تدابير أخرى كمصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع التي تكون محلا للجريمة[2].

الفرع الثاني: الحجز عن طريق منع الوصول إلى المعطيات وحدود استعمالها:

---

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci ou un support de stockage informatique ;

b. réaliser et conserver une copie de ces données informatiques ;

c. préserver l'intégrité des données informatiques stockées pertinentes ; et

d. rendre inaccessibles ou enlever ces données informatiques du système informatique consulté, convention européenne de la cybercriminalité, Op.Cit,p.10.

[1] أمير فرج يوسف المحامي، الجرائم المعلوماتية على شبكة الانترنيت، دار المطبوعات الجامعية، الإسكندرية، مصر، (ب.س.ط) ص237.

[2] تنص المادة (394 مكرر6) من (ق.ع.ج) على:" مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والوسائل والبرامج المستخدمة مع إغلاق المواقع التي تكون محلا للجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كنات الجريمة قد ارتكبت بعلم مالكها".

عرفنا فيما سبق أن المنظومة المعلوماتية عبارة عن نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، وعليه يعتبر عمل المنظومة المعلوماتية غاية في التعقيد سواء كانت هذه المنظومة تعمل منفردة أو متصلة بأخرى عبر شبكة الإنترنت، لذا تواجه أجهزة البحث والتحري صعوبات أثناء توقيع الحجز عليها نتيجة للتطورات التقنية المتلاحقة في مجال تقنية المعلومات.

أولا: الحجز عن طريق منع الوصول إلى المعطيات: يخلق تتبع المجرم المعلوماتي صعوبات تقنية بالغة تحول أحيانا دون الكشف عنه، وبالتالي إفلاته من العقاب، فإذا أمرت السلطة القضائية المختصة بإجراء تحقيق في جريمة ما يكون المجرم الإلكتروني طرفا فيها، فسيحاول محو آثار جريمته ليصعب على المحققين تعقبه، وبالتالي اختفاء الدليل الرقمي الذي يدينه. لذلك نص المشرع في المادة(07) من القانون رقم:09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:" إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة (06) أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الدخول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها...". حيث تتوافق هذه المادة مع نص المادة (3/19-د) من (إ.أ.م.إ.م) بخصوص حفظ المعطيات المخزنة أو إزالتها أو منع الوصول إليها[1]، وهو نفسه ما نصت عليه المادة (1/27-د) من (إ.ع.م.ج.ت.م) سالفة الذكر.

والملاحظ أن المشرع لم يحدد الأسباب التقنية المانعة للحجز سواء ما تعلق بالمنظومة المعلوماتية نفسها كاستحالة الدخول لوجود كلمة السر أو نظام حماية يصعب اختراقه، لأن نظم الحواسيب الحديثة يغلب أن تكون جزء من شبكات واسعة ومعقدة يصعب على السلطات المختصة مباشرة الحجز دون تعاون كامل *(full co-operation)* من القائم على تشغيل النظام[2]، أو ما تعلق بعملية نسخ المعطيات بسبب التطور الدائم في هذه التقنيات، وما يتطلبه ذلك من متابعة وتكوين دوري لأعضاء الأجهزة القضائية المختصة في مجال التحقيق والكشف عن الجرائم المعلوماتية. لذلك

---

[1] ***Article 19 – Perquisition et saisie de données informatiques stockées***

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :...

d. rendre inaccessibles ou enlever ces données informatiques du système informatique consulté..., convention européenne de la cybercriminalité, Op.Cit,p.10.

[2] هشام محمد فريد رستم، الجوانب الإجرائية، المرجع السابق، ص98.

نص على ضرورة إجراء تدابير إحترازية من طرف المختصين باستعمال الوسائل التقنية المناسبة القصد منه عدم تمكين المجرم من الوصول للمعطيات المخزنة في المنظومة المعلوماتية لاستعمالها أو نسخها أو الاطلاع عليها، لأن هذه المعطيات تشكل محل الجريمة تحتوي على أدلة قد يتمكن المجرم من تهريبها أو تدميرها[1].

ثانيا: حدود استعمال المعطيات: تطرقنا فيما سبق إلى أن إجراء مراقبة الاتصالات الإلكترونية يمس بحق الأشخاص في سرية مراسلاتهم ومنها المراسلات الإلكترونية، وهو حق مكفول دستوريا، لذا نص المشرع الجزائري تحت طائلة العقوبات على حدود استعمال المعلومات المتحصل عليها من عمليات المراقبة، إلا فيما تتطلبه التحريات والتحقيقات القضائية، وهذا بموجب نص المادة (09) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الإتصال ومكافحتها:" تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون،إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية".

في هذا الشأن نصت المادة (85) من (ق.إ.ج.ج) على:" يعاقب بالحبس من شهرين إلى سنتين و بغرامة من 2000 إلى 20.000 دينار كل من أفشى أو أذاع مستندا متحصلا من تفتيش شخص لا صفة له قانونا في الاطلاع عليه، وكان ذلك بغير إذن من المتهم أو من خلفه أو من الموقع بإمضائه على المستند أو الشخص المرسل إليه وكذلك كل من استعمل ما وصل إلى علمه ما لم يكن ذلك من ضروريات التحقيق القضائي". وهو مسلك حسن من المشرع الجزائري خاصة فيما يتعلق بمكافحة الجرائم الإلكترونية، حيث توفر تقنية المعلومات المدعمة بشبكة الإنترنت إمكانية هائلة لتبادل ونشر المعلومات بين الأفراد مما قد تكون عرضة لإساءة استخدامها.

من خلال ما سبق ذكره، نص المشرع الجزائري على إجراء تفتيش المنظومة المعلوماتية وحجز المعطيات، وهذا تماشيا مع التشريعات الحديثة والاتفاقيات المبرمة في هذا المجال، رغم صعوبة البحث والتحري عن الجرائم الإلكترونية بسبب التطورات التقنية المذهلة الحاصلة في مجال الحوسبة ونظم الاتصالات، مما يخلق معه صور وأنماط مستحدثة لجرائم جديدة، فهي جرائم حديثة تقع في بيئة افتراضية يصعب اكتشافها والتحقيق فيها وبالتالي يسهل على المجرم المعلوماتي الإفلات من العقوبة. وعليه لا بد من الاهتمام بالتكوين النظري والتدريب العملي للمكلفين من السلطة القضائية المختصة بالتحريات والتحقيقات في الجرائم الإلكترونية قصد اكتساب المهارات الفنية اللاّزمة ومسايرة التطورات التقنية المتلاحقة.

---

[1] زيدان زيبحة، المرجع السابق، ص153.

وكما أوردنا سابقا أن من خصائص الجرائم الإلكترونية أنها جرائم عابرة للحدود، تتطلب تظافر جهود كافة الدول لمكافحتها، لذا عملت هذه الدول على توطيد التعاون والتنسيق فيما بينها لوضع حد لها، وهذا ما عمل عليه المشرع الجزائري في سياسته الجنائية في مجال التعاون والمساعدة القضائية الدولية والذي نوضحه في المبحث الموالي.

المبحث الثالث: في مجال التعاون والمساعدة القضائية الدولية

فرضت الطبيعة الخاصة للجريمة الإلكترونية على الدول التعاون فيما بينها سواء عن طريق الاتفاقيات الدولية كاتفاقيات الأمم المتحدة، أو عن طريق الاتفاقيات الإقليمية مثل: (إ.أ.م.إ.م) والمنظمات الشرطية التابعة لها كمنظمة الإنتربول والأرجست أو خطة العمل المشتركة لإنترنت مضمون*(Safer Internet Action Plan)* بهدف تجاوز تحديات جرائم الكمبيوتر والإنترنت[1]، ففي عام 1983 أجرت منظمة التعاون والإنماء الاقتصادي دراسة حول إمكان تطبيق القوانين الجنائية الوطنية وتكييف نصوصها لمواجهة تحديات الجرائم الإلكترونية. وفي عام 1985 أصدرت هذه المنظمة تقريرا يتضمن قائمة بالحد الأدنى لعدد الأفعال المتعلقة بإساءة استخدام الحاسب الآلي التي يجب علي الدول أن تجرمها وتفرض لها عقوبات في قوانينها، ومن أمثلة هذه الأفعال : الغش أو التزوير في الحاسب الآلي، تغيير برامج الحاسب الآلي أو المعلومات المخزنة فيه ، سرقة الأسرار المدعمة في قواعد الحاسب الآلي، تفعيل التعاون الدولي في مجال مكافحة الجريمة الإلكترونية[2].

وعليه لم تتوقف السياسة الجنائية الإجرائية للمشرع الجزائري بخصوص مكافحة الجرائم الإلكترونية داخل الوطن عن طريق الإجراءات المستحدثة في مجال البحث والتحري، وكذا تمديد الاختصاص للسلطات المكلفة بالتحريات والتحقيقات، إضافة إلى القواعد الإجرائية بموجب القانون رقم:09-04، وإنما امتدت خارج الوطن لتشمل التعاون الدولي وطلبات المساعدة القضائية تنفيذا للتوصيات الدولية بضرورة تظافر جهود الدول لمكافحة الجرائم العابرة للحدود ومنها الجرائم الإلكترونية، وهذا ما أكّدت عليه المادة (30) وما بعدها من (إ.ع.م.ج.ت.م) حول الاختصاص القضائي وتسليم المجرمين[3] والمساعدة القضائية المتبادلة والإجراءات المتعلقة بطلب المساعدة القضائية الدولية...إلخ[1].

---

[1] *CHRISTIANE FERAL-SCHUHL, Le Droit à L'épreuve , Quatrième édition, Op.Cit,pp.664-665.*

[2] مفتاح بوبكر المطردي، المرجع السابق، ص28.

[3] يمثل تسليم المجرمين مظهرا من مظاهر التعاون الدولي في مكافحة ظاهرة الإجرام ، فتقوم دولة من الدول بمطالبة دولة أخرى بتسليمها شخصا ينسب إليه ارتكاب جريمة أو صدر حكم بالعقوبة ضده حتى تتمكن الدولة الطالبة - باعتبارها صاحبة الاختصاص - من

سنتناول التعاون القضائي في الجرائم الإلكترونية في (المطلب الأول)، ثم نتطرق إلى المساعدة القضائية الدولية المتبادلة والقيود الواردة عليها في (المطلب الثاني)، لنتحدث بعدها عن بعض المشكلات التي تواجه سلطات البحث والتحري لمكافحة الجريمة الإلكترونية في (المطلب الثالث).

المطلب الأول: التعاون القضائي

يتيح الفضاء السبراني ارتكاب الجريمة الإلكترونية من أقصى بقاع الأرض السهولة نفسها لارتكابها من أقرب مكان، وعليه فإن موضوع الاختصاص القضائي في الجريمة الإلكترونية وفي ظل الطبيعة الخاصة لهذه الأخيرة التي تتم في بيئة افتراضية لا تعترف بالحدود الجغرافية، يثير مسألة الاختصاص القضائي سواء على المستوى الداخلي للدولة أو الدولي. يعني ذلك تنازع الاختصاص المحلي بين أكثر من جهة قضائية داخل الدولة، إضافة إلى تنازع الاختصاص الدولي بين أكثر من دولة. والذي يطرح مسألة تحديد القانون الواجب التطبيق على هذه الجريمة، فقواعد الاختصاص القضائي التقليدية صيغت لكي تحدد الاختصاص المتعلق بجرائم قابلة للتحديد المكاني للجريمة وهي قواعد ترتكز على مبدأ الإقليمية، وهو ما يرتبط بسيادة الدولة على إقليمها، فلا يكون الخروج عليه بقبول اختصاص قضائي أجنبي إلا في حالات استثنائية يجب النص عليها صراحة[2].

وعليه يُثار التساؤل عن مدى إمكانية الاعتماد على هذه القواعد لتحديد الاختصاص القضائي لجريمة ترتكب في مجال افتراضي لا يعترف بالحدود الجغرافية أو ما يعرف بـ: "لا مركزية الفضاء الشبكي"[3]، وكثيرا ما يكون مرتكبوها في بلاد مختلفة ومن جنسيات متعددة، إضافة إلى تعلق السلوك الإجرامي بأكثر من دولة.

محاكمته أو من تنفيذ العقوبة الصادرة في حقه . ويستمد النظام القانوني لتسليم المجرمين مصدره أحيانا من أحكام التشريع الوطني، ولكن الغالب يكون مصدره الاتفاقيات الدولية أو شبه الدولية أو الثنائية ، وقد يستند التسليم إلى قواعد العرف الدولي أو اتفاق المعاملة بالمثل . والتسليم أكثر جدوى لإدارة استراتيجية مكافحة الجرائم الإلكترونية ، ولا تتأكد فعاليته إلا بتحقق أمرين أولهما :

- تجاوز اعتبارات السيادة القضائية ولو بقدر ضرورات التعاون الدولي.
- قيام التشريعات الوطنية بتفعيل هذا التعاون وتنظيمه وفق ما تقتضيه المعاهدات الدولية ذات الصلة، راجع، مفتاح بوبكر المطردي، المرجع نفسه، ص24.

[1] تنص المادة (32) من (إ.ع.م.ج.ت.م) تحت عنوان: "المساعدة المتبادلة" على: "على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم ملومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم...".

[2] يوسف المصري، المرجع السابق، ص97.

[3] أدت تكنولوجيات الإعلام والاتصال إلى فقدان الحدود الجغرافية كل أثر لها في الفضاء الشبكي أو الآلي، فهو لا يعترف بالحدود الجغرافية، حيث يتم تبادل البيانات في شكل حزم إلكترونية توجه إلى عنوان افتراضي ليس له صلة بالمكان الجغرافي ، فهو فضاء ذو طبيعة لا مركزية إذا يمكن إجمال أهم خصائصه في عدم التبعية لأي سلطة حاكمة. فالفضاء الشبكي هو نظام إلكتروني معقد لأنه عبارة عن شبكة اتصال لا متناهية غير مجسدة وغير مرئية متاحة لأي شخص حول العالم وغير تابعة لأي سلطة حاكمة. فالسلوك المرتكب

وفي ظل هذه الإشكالات المطروحة، يمكن طرح السؤال الآتي: كيف عالج المشرع الجزائري إشكالية الاختصاص القضائي في الجرائم الإلكترونية على المستوي الخارجي؟.

سنتناول بعض صور التعاون القضائي في مكافحة الجريمة بشكل عام في (الفرع الأول)، ثم نتطرق إلى الاختصاص القضائي الدولي الذي ينعقد للمحاكم الجزائرية بخصوص الجرائم الإلكترونية في (الفرع الثاني).

الفرع الأول: صور التعاون القضائي في مكافحة الجريمة بشكل عام:

يعرف التعاون الأمني بين الدول على أنه:" مجموعة الإجراءات التي تتخذها سلطة دولة ما أو جهاز منظمة دولية حكومية بناء على طلب دولة أو منظمة دولية أخرى سواء كانت إجراءات في المجال القضائي أو القانوني الشرطي استنادا إلى المصادر القانونية الدولية المختلفة بهدف المساعدة في مكافحة الجريمة بصفة عامة والجرائم ذات الطابع الدولي بصفة خاصة"[1]. من جهة ثانية حثّ قرار الأمم المتحدة رقم:88/52 بتاريخ:1998/02/04 تحت عنوان:" التعاون الدولي في المسائل الجنائية" على أن معاهدات الأمم المتحدة بشأن التعاون الدولي في المسائل الجنائية توفر أدوات مهمة لأجل تطوير التعاون الدولي بما يسهم في زيادة الكفاءة في مكافحة الإجرام". كما تضمنت أيضا (إ.أ.م.إ.م) على مجموعة من الإجراءات الهامة بخصوص التعاون الدولي في مكافحة الجريمة الإلكترونية[2].

كما تبرز أهمية التعاون القضائي في مجال مكافحة الجرائم عبر الوطنية ومنها الجرائم الإلكترونية، في تميز هذه الأخيرة بخاصية عدم الاعتراف بالحدود الجغرافية، فهي تتحرك في فضاء شبكي يصعب معه ملاحقة المجرمين، مما فرض حتمية التعاون الدولي لأنه شبه مستحيل مكافحة هذا الصنف من الجرائم دون تعاون دولي حقيقي وفعّال على جميع الأصعدة، سواء على مستوى التجريم والعقاب أو على مستوى الإجراءات، ناهيك عن تطوير آليات الملاحقة القضائية الوطنية والدولية من خلال إحداث مؤسسات متخصصة في هذا المجال مثل: الإنتربول والمحكمة الجنائية

فيها يتجاوز الأماكن بمعناه التقليدي، وله وجود حقيقي وواقعي لكنه غير محدد المكان. فالشبكة عالمية النشاط والخدمات لا تخضع لأي قوة مهيمنة إلا في بدايتها حيث كان تمويل هذه الشبكة حكوميا يعتمد على المؤسسة العسكرية الأمريكية، أما الآن فقد أصبح التمويل يأتي من القطاع الخاص حيث الشركات الإقليمية ذات الغرض التجاري التي تبحث عن كافة السبل للاستفادة من خدماتها بمقابل مالي. راجع منير محمد الجنبيهي وممدوح محمد الجنبيهي، المرجع السابق، ص9.

[1] القحطاني خالد بن مبارك القروي، التعاون الأمني الدولي ودوره في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه، قسم فلسفة العلوم الأمنية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2006، ص38.

[2] المواد: (20و24و25و31) من (إ.أ.م.إ.م) .

الدولية...إلخ[1]. في هذا الصدد نصت (إ.أ.م.إ.م) في مادتها (23) على ضرورة تتعاون الأطراف وفقا لأحكام هذا الاتفاقية، وتطبيق القواعد الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية، ووضع ترتيبات ضمن التشريعات والقوانين الوطنية، لتحقيق أقصى حد ممكن من التعاون مع الدول الأخرى لغرض تسهيل التحقيق أو الإجراءات المتعلقة بالجرائم المتعلقة بأنظمة الكمبيوتر والبيانات أو لجمع الأدلة في شكل إلكتروني من جريمة جنائية[2].

حيث بدأ هذا التعاون الدولي يؤتي أُكُله، وخير دليل على المستوى الوطني، هو تمكن مصالح الأمن بعنابة خلال سنة 2016 من ضبط قائمة المشتبه في تكوينهم "شبكة إلكترونية جهادية في الجزائر"، وذلك على إثر إصدار أوامر بالقبض دولية "النشرية الحمراء" في إطار التعاون القضائي الدولي عن طريق المنظمة الدولية للشرطة الجنائية *(INTERPOL)* لملاحقة والقبض على المتورطين في هذا القضية[3].

وفيما يلي نتطرق أولا وبإيجاز لأهم الأجهزة الشرطية الدولية القائمة على مكافحة جرائم الكمبيوتر والإنترنت، وثانيا إلى أبرز صور هذا التعاون القضائي.

أولا: الأجهزة الشرطية الدولية القائمة على مكافحة جرائم الكمبيوتر والإنترنت: سنتناول أهمها وفق ما يأتي:

---

[1] *David Bénichou, Cybercriminalité : jouer d'un nouvel espace sans frontière, Actualité Juridique Pénal, Editions Dalloz, 2009,pp224-226.*

[2] ***Article 23 – Principes généraux relatifs à la coopération internationale***

"Les Parties coopèrent conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible les unes avec les autres, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves sous forme électronique d'une infraction pénale", convention européenne de la cybercriminalité, Op.Cit,p.13.

[3] في هذا الشأن، أصدرت مصالح الأمن بعنابة، فور ضبطها قائمة المشتبه في تكوينهم "شبكة إلكترونية جهادية في الجزائر"، أوامر دولية بالقبض "النشرية الحمراء" في إطار التعاون القضائي الدولي عن طريق المنظمة الدولية للشرطة الجنائية الإنتربول لملاحقة والقبض على المتورطين في الملف، خاصة الجزائريين الذين وردت أسماؤهم ضمن تحقيق خلية مكافحة الجريمة الإلكترونية بأمن عنابة. حيث تم استغلال جميع المعطيات الإلكترونية الخاصة بالمنظومة الآلية للمعطيات الإلكترونية عبر صفحات التواصل الاجتماعي "فايسبوك" للتونسيين والجزائري الموقوفين عبر مطاري قسنطينة وعنابة، ما أسفر عن تحديد هوية "الإرهابيين الجزائريين" المتواجدين حاليا في سوريا للجهاد في صفوف تنظيم "داعش"، من بينهم شباب ينحدرون من عنابة والطارف، لأكثر تفاصيل، الخبر منشور على الموقع الرسمي لوكالة الأنباء الجزائرية:*http://www.aps.dz/ar* تاريخ الاطلاع:2016/10/14 على الساعة:17:00.

1- **المنظمة الدولية للشرطة الجنائية (*INTERPOL*):** وهي أكبر منظمة شرطة دولية أنشئت سنة 1929 مكونة من قوات الشرطة لـ 190 دولة، ومقرها الرئيس في مدينة ليون بفرنسا. ويسعى الإنتربول لضمان حصول أجهزة الشرطة في أرجاء العالم كافة على الأدوات والخدمات اللاّزمة لها لتأدية مهامها بفعالية. ويوفر تدريبا مُحدد الأهداف ودعما متخصصا لعمليات التحقيق ويضع بتصرف الأجهزة المعنية بيانات مفيدة وقنوات اتصال مأمونة. وهذه المجموعة المتنوعة من الأدوات والخدمات تساعد عناصر الشرطة في الميدان على إدراك توجهات الإجرام على نحو أفضل وتحليل المعلومات وتنفيذ العمليات، وفي نهاية المطاف توقيف أكبر عدد ممكن من المجرمين[1].

كما يهدف الإنتربول إلى تسهيل التعاون الدولي بين أجهزة الشرطة حتى في غياب العلاقات الدبلوماسية بين بلدان محددة. ويجري التعاون في إطار القوانين القائمة في مختلف البلدان وبروح الإعلان العالمي لحقوق الإنسان. ويحظر القانون الأساسي للمنظمة أي تحرك أو نشاط ذي طابع سياسي أو عسكري أو ديني أو عنصري[2]. كما يمتلك الإنتربول نظام اتصال حديث يربط الدول الأطراف ويعمل 24/24 ساعة، إضافة إلى قاعدة بيانات للشرطة الجنائية لتبادل المعلومات، ناهيك عن وجود مصالح مختصة تعني بتحليل ظاهرة الإجرام المعلوماتي[3].

2- **الشرطة الدولية للويب (*IWP*):** تم إنشاؤها في عام 1987م، وهي تختص بتحقيق الأمن وإعمال القانون وردع الخارجين عليه وذلك بشعارها الشهير "الخدمة والحماية". ولذلك فإن شرطة الإنترنت تعمل تحت الشعار نفسه بهدف خدمة وحماية مجتمع تكنولوجيا المعلومات وخاصة مجتمع الإنترنت في كافة أنحاء العالم من مخاطر الجرائم الإلكترونية[4].

3- **الأورجست:** وهو جهاز يوجد على المستوى الأوروبي يساعد على التعاون القضائي والشرطي في مواجهة مكافحة جميع أنواع الجرائم الخطيرة للإنترنت، ومن أهم أنشطته تحسين التنسيق والتعاون بين السلطات القضائية المختصة للدول الأطراف وتبادل المعطيات بين الدول أعضاء الاتحاد الأوروبي وإجراء التحقيقات والملاحقات والتبليغ عن الجرائم لدى السلطات المختصة لدى الدول الأطراف وعن التحفظ لديها[5]، ويرمي هذا الجهاز إلى تحقيق ثلاثة أهداف رئيسة هي[6]:

---

[1] *Quéméner (Myriam) et Ferry (Joel), Op.Cit,p.235,voir aussi, David Bénichou, art-Cit,p.230.*

[2] يوسف المصري، المرجع السابق، ص ص100-101.

[3] *Quéméner (Myriam) et Ferry (Joel), Op.Cit,p.236.*

[4] عفيفي كامل عفيفي، المرجع السابق، ص485.

[5] *David Bénichou, art-Cit,p.230.*

[6] *Quéméner (Myriam) et Ferry (Joel), Op.Cit,p.239.*

- تعزيز التعاون بين السلطات القضائية المختصة للدول الأعضاء بخصوص البحث والتحري في مجال مكافحة الجرائم المنظمة ومنها الجرائم الإلكترونية.

- تعزيز التعاون بين الدول الأعضاء في مجال المساعدة القضائية الدولية وتسليم المجرمين.

- مساعدة السلطات القضائية للدول الأعضاء على تحسين فعالية التحقيقات والملاحقات التي تجريها.

4- **مركز الشرطة الأورورببة *(EUROPOL)***: وهي وكالة تطبيق القانون الأوروبية، وظيفتها حفظ الأمن في أوروبا عن طريق تقديم الدعم للدول الأعضاء في الاتحاد الأوروبي في مجالات مكافحة الجرائم الدولية والإرهاب، ومنها جرائم الكمبيوتر والإنترنت. تمتلك الوكالة أكثر من 700 موظف في مقرها الرئيسي الكائن في "لاهاي" في هولندا، وهي تعمل بشكل وثيق مع أجهزة أمن دول الاتحاد الأوروبي ودول من خارج الاتحاد كأستراليا وكندا والولايات المتحدة الأمريكية والنرويج .لا يمتلك ضباط اليوروبول صلاحيات مباشرة للإيقاف والاعتقال ولكنهم يقومون بدعم ضباط الأمن العاديين بالقيام بمهام جمع المعلومات وتحليلها وتوزيعها إضافة لتنسيق المهمات المشتركة، وتستفيد أجهزة الأمن المستقلة لدول الاتحاد بدورها من خدمات الوكالة الاستخباراتية لتجنب وقوع الجرائم وللتحقيق فيها في حال وقوعها ولتعقب وإلقاء القبض على مرتكبيها.

يأتي موظفو اليوروبول من فروع أمنية مختلفة بما في ذلك أجهزة الشرطة العادية وشرطة الحدود وشرطة الجمارك وغيرها. تمتلك الوكالة في مقرها الرئيسي137 ضابطا، يُنتدب هؤلاء الضباط من دول الاتحاد الأوروبي ومن الدول الشريكة للوكالة من خارج الاتحاد. تمت الموافقة على تأسيس اليوروبول في معاهدة ماسترخت عام1992، وباشرت الوكالة بالقيام بعمليات محدودة بتاريخ:03 جانفي1994، وفي عام 1998 تمت مراجعة طبيعة عمل اليوروبول من قبل دول الاتحاد الأوربي وبدأت الوكالة بالقيام بمهامها كاملة بتاريخ :1999/06/01[1].

5- **فضاء شنجن *(Shengen)***: هي المنطقة التي تضم 26 دولة أوروبية، والتي ألغت جواز السفر وضوابط الهجرة على الحدود المشتركة الداخلية بينهما. وهي بمثابة دولة واحدة لأغراض السفر الدولي، مع وجود سياسة تأشيرات مشتركة. وتم إنشاء هذا الفضاء بتاريخ:19 جوان 1990 . ألغت الدول في منطقة شنغن الرقابة على الحدود الداخلية مع أعضاء دول شنغن الأخرى، وتعزيز الرقابة على الحدود الخارجية مع الدول غير الأعضاء في شنغن. يُعد هذا الفضاء أيضا وسيلة هامة لتبادل المعلومات حول الأشخاص المشتبه فيهم بما يخدم أمن الدول الأعضاء وسلامة مواطنيها من

---

[1] طارق إبراهيم الدسوقي عطية، المرجع السابق، ص597، راجع أيضا، فريد نعيم جبور، المرجع السابق، ص216، وأيضا، عفيفي كامل عفيفي، المرجع السابق، ص ص485-486.

كافة الجرائم ومنها الجرائم الإلكترونية باعتبارها جرائم عابرة للحدود[1]. وقد استحدث في هذا الفضاء وسيلتين جديدتين لتعزيز التعاون الشرطي الأوروبي وهما مراقبة المشتبه فيهم عبر الحدود وملاحقة المجرمين[2].

6- **مجلس وزراء الداخلية العرب:** وهو الهيئة الرئيسية التابعة لجامعة الدول العربية والتي تنسّق التعاون بين الدول العربية في ميدان الأمن الداخلي ومكافحة الجريمة المنظمة ومنها جرائم تقنية المعلومات، وقد انضمت إليه الجزائر عقب إنشائه سنة 1982.

هذا بالنسبة لأهم الأجهزة الشرطية الدولية القائمة على مكافحة جرائم الكمبيوتر والإنترنت، لكن بالمقابل ما هي أبرز صور التعاون الدولي في هذا الشأن؟.

ثانيا: صور التعاون الدولي في مجال مكافحة جرائم الكمبيوتر والإنترنت: سنتطرق إلى أبرز هذه الصور فيما يأتي:

1- **تبادل المعلومات:** يتمثل هذا الإجراء في تقديم المعلومات والبيانات والوثائق التي لها علاقة بالاستدلال أو التحقيق للسلطة القضائية الأجنبية أثناء نظرها في جريمة ما[3]، حيث تعطي الدول أهمية قصوى لتبادل المعلومات بوصفها وسيلة فعالة لمكافحة الإجرام عموماً، والجريمة المعلوماتية خصوصاً، لما توفره المعلومات الصحيحة والموثوقة من مساندة لأجهزة تنفيذ القوانين في كافة المجالات، بما في ذلك متابعة نشاط المنظمات الإجرامية. لذلك أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين[4]، بتطوير التبادل المنهجي للمعلومات بوصفه عنصراً رئيساً من عناصر خطة العمل الدولية لمنع الجريمة ومكافحتها، وأوصى بأنه على منظمة الأمم المتحدة أن تنشئ قاعدة معلوماتية لإعلام الدول الأطراف بالاتجاهات العالمية في مجال الجريمة .

وهكذا ينبغي للتعاون في المسائل المتعلقة بالجريمة المعلوماتية أن يدعم بتوظيف نظم تبادل المعلومات بين الدول الأعضاء، وتقديم المساعدة التقنية الثنائية والمتعددة الأطراف إلى الدول الأعضاء، باستخدام التدريب على تنفيذ القوانين والمعاهدة المتعلقة بالعدالة الجنائية. وعليه نصت

---

1 *Quéméner (Myriam) et Ferry (Joel), Op.Cit,p.240.*

2 عفيفي كامل عفيفي، المرجع السابق، ص486.

3 طارق إبراهيم الدسوقي عطية، المرجع السابق، ص598.

4 عُقد هذا المؤتمر في كراكاس بفنزويلا سنة 1980 تحت شعار:" الوقاية من الجريمة ونوعية الحياة"، أين عُرضت أول دراسة استقصائية مفصلة تعدها الأمم المتحدة عن الجريمة في مختلف أنحاء العالم, استنادا إلى معلومات واردة من 65 دولة عضوا، وأظهرت تلك الدراسة أن الغالبية العظمى من البلدان المتقدمة والنامية تواجه تصاعدا في العنف والإجرام، وأن الإجرام يتخذ أشكالا وأبعادا جديدة وأن التدابير التقليدية لمنع الجرمة ومكافحتها ليست قادرة على معالجة الوضع، راجع مضمون هذا المؤتمر المنشور على الموقع الرسمي للأمم المتحدة : *http://www.un.org/ar/events/crimecongress2015/about.shtml* ، تاريخ الاطلاع:2016/10/11 على الساعة:17:04.

كثير من الاتفاقيات الدولية على التبادل المنهجي للمعلومات، أهمها معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية[1].

ولا شك أن هذه الصورة من المساعدة القضائية مفيدة للغاية، ونحن بصدد الجرائم الإلكترونية العابرة للحدود، حيث أنه لكشف الجريمة ومرتكبها لابد من توفر معلومات كافية لأجهزة البحث والتحري لملاحقة المجرم المعلوماتي في هذا الفضاء الافتراضي.

2- **الإنابة القضائية:** ويقصد بها:" طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، بهدف الفصل في مسألة معروضة على السلطة القضائية للدولة الطالبة ويتعذر عليها القيام به بنفسها"[2]. كما تنتج الإنابة القضائية عن الواجبات أو الالتزامات التي يفرضها القانون الدولي العام على الدول، وبموجبها يعهد للسلطات القضائية – المطلوب منها اتخاذ إجراء – القيام بالتحقيق أو بالعديد من التحقيقات، لمصلحة السلطة القضائية المختصة في الدول الطالبة، مع مراعاة احترام حقوق وحريات الإنسان المعترف بها عالميا، ومقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل، واحترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القانونية.

وتهدف الإنابة القضائية إلى نقل الإجراءات في المسائل الجنائية، لمواجهة ما تشهده الظواهر الإجرامية من تطور، ناهيك عن طابع السرعة الذي تتطلبه الإجراءات المتعلقة بملاحقة الجريمة الإلكترونية سواء كان ذلك بواسطة الولوج عن بعد في المنظومة المعلوماتية أو تقفي آثار المجرم الإلكتروني لضبط المعلومات محل الجريمة[3]، إضافة إلى تذليل العقبات التي تعرض سير الإجراءات الجنائية المتعلقة بقضايا ممتدة خارج إقليم الدولة التي تمنعها من ممارسة بعض الأعمال القضائية داخل إقليم الدولة الأخرى[4]. كما أن الإنابة القضائية تجد أساسها في القوانين الوطنية، وفي الاتفاقيات الدولية وفي مبدأ المعاملة بالمثل[5].

---

[1] المادة (1) من المعاهدة النموذجية لتبادل المساعدة في المسائل الجنائية والبروتوكول الاختياري بشأن عوائد الجريمة، والتي تحث أطرافها على تقديم كل منهم للآخر أكبر قدر من المساعدة القضائية المتبادلة في التحقيقات أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية في الدولة الطالبة للمساعدة، راجع نص المعاهدة المنشورة على الموقع الرسمي للأمم المتحدة : *http://www.un.org/arabic/documents/basic/treaties.html*، تاريخ الاطلاع:2016/10/11 على الساعة:17:16 .

[2] يوسف المصري، المرجع السابق، ص104.

[3] زيدان زيبحة، المرجع السابق، ص144.

[4] طارق إبراهيم الدسوقي عطية، المرجع السابق، ص601.

[5] حسين بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص646.

3- **تنفيذ الحكم الأجنبي:** من المفاهيم التي يجب تجاوزها لدعم أواصر التعاون الدولي، عدم قابلية الحكم الأجنبي للتنفيذ بحجة أن الحكم الجنائي في حقيقته مظهر لسيادة الدولة ويلحقها في توقيع العقاب، إلا أنه لا ينبغي أن يقتصر الأمر على ما يرتبه الحكم الجنائي الأجنبي من أثار سلبية مثل: عدم جواز محاكمة الشخص على الفعل الواحد مرتين. نتيجة لتلك الجهود تم إبرام العديد من الاتفاقيات الدولية، لتنفيذ الأحكام القضائية بما فيها الأحكام الجنائية لوضع قواعد خاصة لتنفيذ الأحكام الأجنبية كعرض الحكم الأجنبي أمام جهة قضائية وطنية لمنحه الصيغة التنفيذية عندما يستنفذ كافة طرق الطعن ويكون غير مخالف للنظام العام حسب قانون القاضي الآمر بالتنفيذ[1] ، من جانب آخر، ألزمت الاتفاقية التي أبرمت سنة 1952 بين أعضاء الجماعة الأوروبية الدول الأطراف بتنفيذ الأحكام الجنائية وغيرها، ما لم تؤدي إحدى الحالات المحددة حصراً للامتناع عن تنفيذه، ونصت على الأمر نفسه المادة (03) من اتفاقية مكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية 1988.

الفرع الثاني: الاختصاص القضائي الدولي:

تُثار مشكلة الاختصاص القضائي الدولي بالنسبة للجرائم الإلكترونية بصورة أكبر، مما هي عليه داخل إقليم الدولة، حيث بإمكان الدولة سن تشريعات وطنية تعالج المشكلة داخل النطاق الإقليمي لها، وهذا بخلاف معالجة الأمر على المستوى القضائي الدولي، لأن من طبيعة الجرائم الإلكترونية أنها لا تعترف بالحدود الجغرافية للدول، كما يصعب عليها بمفردها مواجهة الجرائم الإلكترونية. فقد تخضع الجريمة للاختصاص الجنائي للدولة بناء على مبدإ الإقليمية، كما قد تخضع لاختصاص دولة أخرى على أساس مبدإ الاختصاص الشخصي، في حين يمكن تمس الجرائم الإلكترونية بأمن وسلامة الاقتصاد الوطني للدولة، فحينئذ يؤول الاختصاص القضائي لهذه الدولة استنادا لمبدإ العينية[2].

تناولنا سابقا مسألة الاختصاص القضائي للسلطات المكلفة بالتحريات والتحقيقات بخصوص الجريمة الإلكترونية، والتي لا تثير أي اشكال على الصعيد الوطني، حيث قام المشرع الجزائري بتمديد الاختصاص المحلي للسلطات القضائية سواء النيابة العامة أو التحقيق أو جهة الحكم ليشمل كافة الإقليم الوطني، لكن المشكلة تظهر بخصوص البحث والتحقيق خارج الإقليم الوطني على أساس عولمة الجريمة الإلكترونية وارتباطها بمجالات عديدة كالتعامل التجاري والمالي على شبكة الإنترنت وانتشار التجارة الإلكترونية وأنظمة الدفع الالكتروني، وما قد ينتج عن هذه العمليات من جرائم مثل:

---

[1] الطيب زروتي، القانون الدولي الخاص الجزائري مقارنا بالقوانين العربية، مطبعة الكاهنة، الجزائر، ج1، 2000، ص21.

[2] طارق ابراهيم الدسوقي عطية، المرجع السابق، ص593، راجع أيضا، فايز محمد راجح غلاب، الأطروحة السابقة، ص379.

الاحتيال المعلوماتي، وتبييض الأموال...إلخ[1]، وهذا إعمالا لمبدإ العينية[2] بموجب نص المادة (588) من (ق.إ.ج.ج).

في هذا الصدد، بادر المشرع الجزائري بحل هذه المشكلة وذلك بالنص في المادة (15) من القانون رقم:09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الإتصال ومكافحتها التي تنص على: "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للإقتصاد الوطني".

من خلال نص المادة نستنتج الشروط القانونية الواجب توافرها لانعقاد الاختصاص للمحاكم الجزائرية وهي:

- أن يكون الجاني أجنبيا، لأنه لو كان جزائريا لطُبق مبدأ الشخصية سواء بموجب المادة (582) إذا كان الفعل يشكل جناية، أو المادة (583) إذا كان الفعل يشكل جنحة.
- أن ترتكب الجريمة في الخارج، لأنه لو ارتكبت في الوطن فيطبق مبدأ الإقليمية.
- على أن توصف الجريمة على أنه جناية أو جنحة.
- أن تستهدف هذه الجريمة مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للإقتصاد الوطني.
- أن تحصل الجزائر على تسليمه لها أو أن يلقى القبض عليه في الجزائر. إذ لا يجب أن يحاكم غيابيا.

- أن تكون الجريمة من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والمنصوص عليها بموجب المواد من(394 مكرر - 394 مكرر7) من (ق.ع.ج).

---

[1] زيدان زيبحة، المرجع السابق، ص175.

[2] مبدأ العينية: هو مبدأ مكمل لمبدإ الإقليمية وسمي أيضا "بمبدأ الذاتية" لأنه يمس بمصالح الدولة ذاتها أو بعينها لا بمصالح أفرادها سواء كانوا جناة أو مجني عليهم، وأنه يطبق خصيصا على الأجانب دون حاملي جنسية الدولة، لأنه هؤلاء يخضعون لمبدإ الشخصية وعموما، نقصد بهذا المبدإ تطبيق القانون الوطني الجزائري على كافة الجرائم المرتكبة بالخارج - لا بأرض الوطن، لأنه في هذه الحالة الأخيرة نطبق مبدأ الإقليمية- والتي تمس بالمصالح الأساسية للدولة المرتبطة بسيادتها واقتصادها والثقة المولاة في نقودها، وأن الضحية في هذا النوع من الجرائم هي الدولة ذاتها، وبهذا المبدإ تكون تمارس نوعا من الدفاع الشرعي عن مصالحها. وهو الأمر الذي دفع بالمشرع الجزائري على غرار غالبية التشريعات الجنائية المعاصرة للنص عليه في (ق.إ.ج.ج) ، عبد المنعم سليمان، النظرية العامة لقانون العقوبات، دار الجامعة الجديدة، الإسكندرية، مصر،2000، ص137.

وعليه يمكن للسلطات القضائية الجزائرية مباشرة الدعوى الجزائية ضد كل شخص أجنبي مشتبه به أو قام بارتكاب الجرائم الإلكترونية التي تهدد مصالح الدولة الجزائرية.

لكن هل اكتفى المشرع الجزائري بتمديد اختصاص المحاكم الجزائرية في هذا الشأن، أم أن المشرع أقر إجراءات أخرى؟ هذا ما سنعرفه في المطلب الموالي.

المطلب الثاني: في مجال المساعدة القضائية الدولية

تتميز شبكة الإنترنت بأنها شبكة عالمية لا تعترف بالحدود الجغرافية، وبالتالي فإن الجرائم المتصلة بها تعتبر هي الأخرى عالمية وذات طابع دولي وأثرها يمتد لأكثر من دولة، وعليه يستلزم ملاحقة مرتكبي هذه الجرائم القيام بإجراءات خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها. ومن هذه الإجراءات معاينة مواقع الإنترنت في الخارج أو ضبط الأقراص الصلبة أو تفتيش نظم الحاسوب، وهذا كله يثير مسألة تحديد قواعد الاختصاص الدولي المنصوص عليه في القوانين الداخلية للدول عند غياب المعاهدات بين الدول المعنية، فمن جهة يؤدي حصر الاختصاص بإقليم دولة ما إلى إمكانية إفلات المجرمين الالكترونيين من العقاب عبر حدود هذه الدولة، ومن جهة أخرى يؤدي عمليا التجريم المتراكم بتطبيق قوانين كل الدول المتصلة بشبكة الإنترنت إلى تجريم الفعل الواحد أكثر من مرة(1).

وعليه لا مناص للدول من تقديم المساعدة القانونية المتبادلة فيما بينها في المسائل الجنائية، إذ تعد من الآليات الفعّالة لمواجهة الجريمة المنظمة العابرة للحدود ومنها الجرائم الإلكترونية، وهو ما يعكسه اهتمام المجتمع الدولي بإبرام المعاهدات والاتفاقيات الثنائية لتسهيل عمل السلطات القضائية المكلفة بالبحث والتحري خاصة ما تعلق بمكافحة جرائم الكمبيوتر والإنترنت بسبب طبيعتها الخاصة.

سنتناول المساعدة القضائية الدولية المتبادلة والقيود الواردة عليها في (الفرع الأول)، ثم نتطرق إلى تبادل المعلومات واتخاذ الإجراءات التحفظية في (الفرع الثاني).

الفرع الأول: المساعدة القضائية الدولية المتبادلة، شروطها والقيود الواردة عليها:

تعتبر المساعدة القضائية الدولية آلية فعّالة في مكافحة الجرائم الإلكترونية، على اعتبار أنها جرائم عابرة للحدود لا تستطيع دولة مكافحتها لوحدها، ورغم ذلك لم يترك المشرع الأمر على اطلاقه بل قيّدها بشروط تبعا لمبدإ سيادة الدولة والمعاملة بالمثل. سنتطرق أولا: لمفهوم المساعدة القضائية الدولية، وثانيا: لشروط المساعدة القضائية المتبادلة.

---

[1] فريد منعم جبور، المرجع السابق، ص205.

أولا: مفهوم المساعدة القضائية الدولية: يمكن تعريف المساعدة القضائية الدولية بأنها:" كل إجراء قضائي تقوم به دولة، من شأنه تسهيل مهمة المحاكمة في دولة أخرى، بصدد جريمة من الجرائم"[1]. من جانب آخر، ركزت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة بتاريخ:2000/11/15 في المادة (18) على المساعدة القانونية المتبادلة وفي المادة (19) على التحقيقات المشتركة بين الدول وفي المادة (20) على أساليب التحري الخاصة لهذا النوع من الجرائم. كما تتخذ المساعدة القضائية صورا عديدة كتبادل المعلومات ونقل الاجراءات والإنابة القضائية الدولية خاصة فيما يتعلق بإجراءات الدخول إلى منظومة معلوماتية بغرض تفتيشها. وعليه تتخذ المساعدة القضائية في المجال الجنائي صورا عديدة نذكر منها:

– **تبادل المعلومات:** ويشمل تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد التحقيق في جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم[2]. كما نصت (إ.أ.م.إ.م) في المادة (46/ب) على ضرورة مشاورة الأطراف فيما بينها حول تبادل المعلومات وكل ما هو جديد في مجال الإجراءات القضائية والجوانب التقنية المتعلقة بمكافحة الجرائم الإلكترونية وجمع الأدلة في الشكل الإلكتروني[3].

– **نقل الإجراءات:** وهو قيام دولة بناء على اتفاقية باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة، وذلك إذا توافرت شروط معينة منها، أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في كلا الدولتين وأن يؤدي الإجراء المطلوب الوصول إلى الحقيقة. وقد أقرّت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى طرق المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة2000، والأمر نفسه نجده في معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لسنة 1999بموجب نص المادة (09) منها. وفي الاتجاه نفسه، أقر المجلس الأوروبي اتفاقية نقل الإجراءات الجنائية التي تعطي للأطراف المنظمة

---

1 خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص407.

2 طارق إبراهيم الدسوقي عطية، المرجع السابق، ص598.

3 ***Article 46 – Concertation des Parties***

1. *"Les Parties se concertent périodiquement, au besoin, afin de faciliter :…*

b. l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique… ", convention européenne de la cybercriminalité, Op.Cit,p.23.

إمكانية محاكمة الجاني طبقا لقوانينها بناء على طلب دولة أخرى طرفا في الاتفاقية، بشرط أن يكون الفعل معاقب عليه في الدولتين[1].

وحسنا فعل المشرع الجزائري في سياسته الجنائية، حينما قام بالتصديق على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[2] خاصة في مجال مكافحة الجرائم الإلكترونية على اعتبار أنه لا يمكن لدولة بمفردها القيام بذلك نظرا للطبيعة الخاصة لهذه الجرائم المستحدثة. من جهة أخرى اتجه المشرع إلى إبرام الاتفاقيات الثنائية في هذا المجال قصد التعاون على مكافحة هذا النوع المستحدث من الجرائم، مثل: إبرام اتفاقيتين ثنائيتين مع فرنسا الأولى سنة 2007 في مجال التعاون في مكافحة الجرائم المنظمة[3]، والثانية بتاريخ: 2016/10/05 بخصوص التعاون القضائي في المجال الجنائي والمتعلقة بمكافحة الجريمة المنظمة العابرة للأوطان ومنها الجرائم الإلكترونية بكافة أشكالها[4].

---

1 يوسف المصري، المرجع السابق، ص104

2 المواد (20-18) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم:2000/11/15، صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم:02-55 المؤرخ في:2002/02/05، (ج. ر) رقم:09 المؤرخة في:2002/02/10، ص 71 وما بعدها.

3 في هذا الشأن أبرمت الجزائر وفرنسا اتفاقية ثنائية حول التعاون في مكافحة الجرائم المنظمة، وذلك بموجب المرسوم الرئاسي رقم:07-375 المؤرخ في:2007/12/01.

4 تم التوقيع على هذه الاتفاقية بباريس بتاريخ: 2016/10/05، وهي تخص التعاون القضائي في المجال الجنائي بين البلدين، تسمح للجزائر وفرنسا بتعزيز تعاونهما في مجال مكافحة الجريمة المنظمة العابرة للأوطان. ومنها الجرائم الإلكترونية. وقّع على الاتفاقية كل من وزير العدل حافظ الأختام السيد: (الطيب لوح) ونظيره الفرنسي (جون جاك إيرفواس) عقب المحادثات التي توسّعت إلى أعضاء وفدي البلدين. وتأتي الاتفاقية لتعوض اتفاق 28 أوت 1962 في شقها الجنائي. حيث تم التفاوض على هذه الاتفاقية مع احترام سيادة البلدين وأخذ خصوصيات الأنظمة القانونية والقضائية لكلاهما بعين الاعتبار، فضلا عن الأحكام المتعلقة بتبليغ الاستدعاءات وتنفيذ الإنابات القضائية. كما تتضمن الاتفاقية أحكاما جديدة تتعلق بسماع المتهمين والشهود عن طريق تقنية المحادثة المرئية عن بعد والتسليم المراقب للوثائق والمعلومات عبر الطريق الالكتروني، لأكثر تفاصيل، راجع الموقع الرسمي لوكالة الأنباء الجزائرية على الرابط الآتي: *http://www.aps.dz/ar/economie/34634-%D8%A7%D9%84%D8%AC%D8%B2%D8%A7%D8%A6%D8%B1-%D9%81%D8%B1%D9%86%D8%B3%D8%A7-%D8%A7%D9%84%D8%AA%D9%88%D9%82%D9%8A%D8%B9-%D8%A8%D8%A8%D8%A7%D8%B1%D9%8A%D8%B3-%D8%B9%D9%84%D9%89-%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D8%A9-%D8%AA%D8%B9%D8%A7%D9%88%D9%86-%D9%82%D8%B6%D8%A7%D8%A6%D9%8A-%D9%81%D9%8A-%D8%A7%D9%84%D9%85%D8%AC%D8%A7%D9%84-%D8%A7%D9%84%D8%AC%D9%86%D8%A7%D8%A6%D9%8A*، تاريخ الاطلاع:2016/10/07 على الساعة:09:09.

ثانيا: شروط المساعدة القضائية المتبادلة: تنفيذا للالتزامات الدولية للجزائر في هذا الشأن خاصة ما تعلق بإجراء التحقيقات والتحريات في مجال الجرائم المعلوماتية والكشف عن مرتكبيها نص المشرع في المادة (1/16) من القانون رقم:09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على: "في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني. يمكن في حالة الاستعجال ومع مراعات الاتفاقيات الدولية ومبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها".

حيث تؤكد المادة (16) سالفة الذكر على أنه وفي إطار التحقيقات والتحريات التي تمت مباشرتها بخصوص الجرائم الإلكترونية، فيمكن للسلطات القضائية المختصة تبادل المساعدة القضائية على المستوى الدولي قصد جمع الأدلة الخاصة بالجريمة الإلكترونية على أساس ما تشكله هذه الجرائم المستحدثة من صعوبات تقنية بالغة على مستوى كشفها وإثابتها وملاحقة مرتكبيها، إذ لا يمكن لدولة بمفردها القيام بذلك. ونظرا لحالة الاستعجال التي تتطلبها إجراءات التحقيق وجمع الأدلة الخاصة لهذا النوع من الجرائم المستحدثة وما يتطلبه من سرعة لاتخاذ هذه الاجراءات، أقر المشرع قبول طلبات المساعدة القضائية حتى وإن جاءت عن طريق وسائل الاتصال السريعة كالبريد الإلكتروني أو الفاكس بشرط التأكد من صحتها فقط . وعليه تتم المساعدة القضائية الدولية بشروط هي:

- تتم وفق الاتفاقيات الدولية التي أبرمت في مجال تبادل المعلومات واتخاذ الإجراءات التحفظية أو تسليم المجرمين فيما يتعلق بمكافحة الجرائم الإلكترونية.
- تخضع لمبدإ المعاملة بالمثل، احتراما لمبدإ سيادة الدولة.

في هذا المجال نصت المادة (36) من الأمر رقم: 05- 06 المؤرخ في:2005/08/23 يتعلق بمكافحة التهريب تحت عنوان "التعاون العملياتي" على:" مع مراعاة مبدإ المعاملة بالمثل، وفي إطار الاتفاقيات الثنائية ذات الصلة، توجه طلبات المساعدة في مجال محاربة التهريب الصادرة عن السلطات الأجنبية كتابيا، أو بالطريقة الإلكترونية إلى الجهات المختصة، وتكون مصحوبة بكل المعلومات الضرورية. إذا ما وُجّه الطلب إلكترونيا يمكن تأكيده بواسطة أي وسيلة تترك أثرا

مكتوبا..."[1]. وعليه لا يمثل استعمال جهاز الفاكس مشكلة إذ يُحوّل آليا البيانات الواردة إليه في الشكل الإلكتروني إلى نص مطبوع على الورق، أما بالنسبة لاستعمال البريد الالكتروني*(e-mail)* فلا مشكلة أيضا، إذ توفر تقنية المعلومات إمكانية طبع أي نص يكون في الشكل الإلكتروني ليصبح مستندا ورقيا.

لقد وُفّق المشرع الجزائري في تسهيل قبول طلبات المساعدة القضائية باعتماد الطلب حتى وإن جاء عبر وسائل تكنولوجيات الإعلام والاتصال الحديثة بشرط التأكد من صحته، وهذا بسبب السرعة المتطلبة للبحث والتحري عن الجرائم الإلكترونية -ذات الطبيعة الخاصة- وملاحقة المجرم الإلكتروني ضمانا لعدم إفلاته من العقاب.

وهذا ما مكّن سلطات البحث والتحري الجزائرية بالتعاون مع السلطات الألمانية وسفارة الولايات المتحدة الأمريكية بالجزائر ومكتب الإنتربول *(Interpol)* فرع بالجزائر، من القبض على الرأس المدبر للشبكة الإجرامية المختصة في القرصنة الإلكترونية، حيث قام هذا الشخص وهو من مدينة عنابة باختراق قاعدة بيانات متواجدة بمدينة ميونيخ بألمانيا وقام بتحميل البيانات الرقمية الخاصة بـ15000 بطاقة إئتمان باستعمال عنوان إلكتروني*(Adresse IP)*، مما مكّنه من تحويل ما قيمته 100.000دولار منذ سنة 2005 من حسابات زبائن البنك الكندي *(Caisse Populaire Des Jardins)*. حيث أدانت محكمة عنابة قسم الجنح الجاني بجنحة تصميم وإدخال عن طريق الغش لمعطيات في نظام المعالجة الآلية والمتاجرة فيها أدت إلى تعديل معطيات تلك المنظومة المعلوماتية وكذا جنحة التقليد، ومعاقبته بعام حبسا نافذا وغرامة قدرها 500.000 دج طبقا لنصوص المواد:(394 مكرر1 -394 مكرر2) من (ق.ع.ج) والمواد:(151 و152 و153) من القانون رقم: 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة[2].

تجدر الإشارة إلى أنه يجب أن يشمل التعاون القضائي لمكافحة الجرائم الإلكترونية، تبادل المعلومات، وتسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة صالحة للإثبات في الاتهام أمام محاكم دولة أخرى، ولا يتأتى هذا إلا عن طريق إبرام الاتفاقيات الدولية لضمان محاكمة مجرمي المعلوماتية وتجنب إيجاد ما يسمى بجنة جرائم المعلوماتية *(Computer Crime Havens)*[3].

---

[1] المادة (36) من الأمر رقم:05-06 المؤرخ في: 2005/08/23 يتعلق بمكافحة التهريب،(ج. ر) رقم:59 المؤرخة في:2005/08/28، ص7.

[2] أنظر: الحكم رقم: 10/07357 الصادر عن محكمة عنابة قسم الجنح بتاريخ: 2010/06/28.

[3] يقصد بجنة جرائم المعلوماتية: إيجاد منطقة خالية من التطبيق القانوني على غرار الجنات الضريبية المنتشرة في بعض الدول، حيث يستطيع المجرم الإلكتروني أن يعبث من خلالها بالأنظمة القانونية، ويتحايل على الأحكام العقابية، فيكون من الصعب ملاحقته ومعاقبته طارق إبراهيم الدسوقي عطية، المرجع السابق، ص604.

ولكن على الرغم من أهمية المساعدة القضائية في هذا المجال، يُثار التساؤل الآتي: هل ترك المشرع الجزائري الأمر على إطلاقه، أم أنه وضع قيودا على ذلك؟.

ثالثا: القيود الواردة على طلبات المساعدة القضائية الدولية: إن اللّجوء إلى الإنابة أو المساعدة القضائية الدولية ليست مطلقة وفق المشرع الجزائري، حيث نصت المادة (18) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على: "يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام. يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب".

وعليه يتم رفض طلبات المساعدة القضائية في الحالات الآتية:

- إذا كان فيها مساس بالسيادة الوطنية.
- إذا كانت ماسة بالنظام العام.

كما يمكن الاستجابة لطلبات المساعدة القضائية وذلك بشروط:

- المحافظة على سرية المعلومات المبلغة لتلك الدولة.
- عدم استعمال المعلومات في غير الحالة الموضحة في طلب المساعدة القضائية.

وهذا بسبب حساسية وأمن المعطيات والبيانات التي قد تحتويها منظومة معلوماتية سواء ما تعلق بأن الدولة أو الأشخاص، تجنبا للمشكلات التي تُثار بين الدول في هذا المجال مثل: التجسّس بكافة أشكاله...إلخ. لذا ألزمت الاتفاقية الدولية الموضوعة للتوقيع بمقر الأمم المتحدة في نيويورك في:2005/09/14 والخاصة بقمع أعمال الارهاب النووي الأطراف وفق نص المادة(2/07) منها باتخاذ التدابير لحماية سرية المعلومات التي يحصل عليها سرا بموجب هذه الاتفاقية من دولة لأخرى[1].

الفرع الثاني: تبادل المعلومات واتخاذ الإجراءات التحفظية:

نظرا لما تُثيره مسألة المساعدة القضائية بين الدول من حساسية متعلقة بسيادة الدولة من جهة ومن جهة أخرى بطبيعة جرائم الحاسوب والإنترنت التي يمكن من خلالها الحصول على معلومات تتعلق بأمن الأفراد والدولة على حد سواء، وضع المشرع الجزائري شروطا للمساعدة القضائية ترجمته نص المادة (17) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة

---

[1] المرسوم الرئاسي رقم:10-270 المؤرخ في:2010/11/10 يتضمن التصديق بتحفظ على الاتفاقية الدولية لقمع أعمال الإرهاب النووي المفتوحة للتوقيع في مقر الأمم المتحدة في نيويورك في:2005/09/14، (ج. ر) رقم:68 المؤرخة في:2010/11/10، ص6.

بتكنولوجيات الإعلام والاتصال ومكافحتها التي تنص على: "تتم الاستجابة إلى طلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل". وهذا ما جاءت به أيضا المادة (04) من (إ.ع.م.ج.ت.م) التي تنص على: "تلتزم كل دولة طرف وفقا لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى. ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي".

من خلال نص المادة (17) سالفة الذكر، نستنتج الشروط الواجب توافرها لتنفيذ طلبات المساعدة لتبادل المعلومات وكذا الإجراءات التحفظية، تتمثل هذا الشروط في:

- تكون وفقا للاتفاقيات الدولية المبرمة في مجال مكافحة الجرائم المعلوماتية، وما يرتبط بها كتبادل المعلومات وتسليم المجرمين والإنابة القضائية...إلخ.
- خضوعها لمبدإ المعاملة بالمثل الذي يؤكد سيادة الدولة، وهو المبدأ الذي أكدته أيضا المادة (29) من القانون رقم:05-01 المؤرخ في:2005/02/26 والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحته، إذ تنص على:" يتم التعاون القضائي بين الجهات القضائية الجزائرية والأجنبية خلال التحقيقات والمتابعات والإجراءات القضائية المتعلقة بتبييض الأموال وتمويل الإرهاب، مع مراعاة المعاملة بالمثل وفي إطار احترام الاتفاقيات الثنائية والمتعددة الأطراف المطبقة في هذا المجال والمصادق عليها من قبل الجزائر طبقا للتشريع الداخلي".

- توفر شروط أمن كافية للتأكد من صحة المعلومات الواردة عن طريق وسائل الاتصال الحديثة.

لقد وضع المشرع الجزائري هذه الشروط طبقا لمبدإ المعاملة بالمثل واحتراما للسيادة الوطنية وأيضا حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي وفقا لنص المادة (46) من القانون رقم: 16-01 يتضمن التعديل الدستوري، وما تمثله هذه المعلومات من خطورة على سلامة الشخص أولا، وعلى أمن الدولة ثانيا، ناهيك عما تثيره مسألة تبادل المعلومات من حساسية بين الدول خاصة في ظل الاتجاه الدولي لمكافحة كافة أشكال الإرهاب ومنها الإرهاب الإلكتروني، حيث تتطلب هذه العملية تبادل المعلومات بين الدول فيما يخص مواطنيها المشتبه فيهم أو المتهمين بالإرهاب، وما يتخلله ذلك من بعض الخروقات التي تؤدي إلى المساس بحقوق الانسان ومنها الحق في الخصوصية والحقوق المتفرعة عنها.

وفي الأخير وبرغم النصوص القانونية التي وضعها المشرع لمواجهة هذا النوع المستحدث من الجرائم، لازالت هناك صعوبات موضوعية وأخرى إجرائية تواجه سلطات البحث والتحري على أساس أنها الواجهة الأولى للتعامل مع هذه الجرائم في عالم افتراضي مفتوح على كافة الحدود ويتسم بالديناميكية والتطور المستمر، هذا ما سنتطرق إليه في المطلب التالي.

المطلب الثالث: الصعوبات التي تواجه سلطات البحث والتحري في مواجهة الجرائم الإلكترونية

إذا كانت الجرائم الإلكترونية أثارت مشكلات فيما يتعلق بجانب التجريم والعقاب، تمثل في إمكانية تطبيق النصوص التقليدية على هذا النوع المستحدث من الجرائم، فقد أثارت في الوقت نفسه العديد من المشكلات في نطاق القانون الجنائي الإجرائي، حيث وضعت نصوص قانون الإجراءات الجنائية لتحكم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها مع خضوعها لمبدإ حرية القاضي الجنائي في الاقتناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم.

وباعتبار أن السلطات القضائية المكلفة بالتحريات والتحقيقات هي الواجهة الأولى في مكافحة الجريمة الإلكترونية، إذ يُلقى على عاتقها كشف الجريمة وتقديم المجرم الإلكتروني لينال جزاءه، تجد صعوبات موضوعية وإجرائية بالغة في القيام بهذه المهمة نظرا للطبيعة الخاصة لهذه الجرائم. سنتناول الصعوبات الموضوعية التي تعيق سلطات البحث والتحري في الكشف عن الجرائم الإلكترونية في (الفرع الأول)، ثم نتطرق إلى الصعوبات الإجرائية التي تصعب من عملهم في (الفرع الثاني).

الفرع الأول: الصعوبات الموضوعية:

نتيجة لإساءة استخدام تكنولوجيا الإعلام والاتصال، تُعد الجريمة الإلكترونية من أكبر التحديات التي تواجهها الدول في عصرنا اليوم، حيث باتت تتخذ أنماطا جديدة وضربا من ضروب الذكاء الإجرامي، بما يعني التشخيص الأمثل للظاهرة ومكافحتها على صعيد التجريم والعقاب، يمكن تلخيص أهم هذه الصعوبات في ما يلي:

أولا: الطبيعة المستحدثة للجرائم الإلكترونية: أدت الثورة التكنولوجية الحديثة في مجال صناعة الحوسبة والاتصال إلى انتشار التقنية المعلوماتية في شتى مجالات الحياة، حيث صار من الصعب الاستغناء عن الحاسوب أو الهاتف النقال في القيام بأعمالنا اليومية، لكن بالمقابل أدى سوء استخدام هذه التقنية إلى بروز نوع مستحدث من الجرائم، تسمى بالجرائم الإلكترونية أو المعلوماتية. وعليه تدخل الجرائم الإلكترونية في نطاق الظاهرة الإجرامية المستحدثة، بالنظر إلى أن أول حالة موثقة لجريمة إلكترونية تعود لعام 1959 وبالنظر لنحو 36 عاما من التعايش الدولي مع صور مختلفة من

هذ الجرائم مثل: جرائم تنصب على معطيات الحاسوب (بيانات ومعلومات وبرامج...إلخ) وتطال الحق في المعلومات، ويستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسوب بوصفه نظاما حقق التزاوج بين تقنيات الحوسبة والاتصال. ونظرا لهذه الطبيعة المستحدثة فإن وسائل مكافحتها لاتزال متأخرة بالمقارنة بوسائل مكافحة الجرائم التقليدية بسبب التأخر في وضع الإطار التشريعي في كثير من الدول لمكافحة هذا النوع من الجرائم[1]، مما يخلق صعوبات بالغة لأجهزة البحث والتحري في التعامل معها في ظل نقص الوسائل التقنية المستعملة، إضافة إلى نقص الخبرة لدى أعضاء الضبط القضائي .

بالنسبة للمشرع الجزائري كان أول إطار قانوني وضعه لمكافحة هذه الجرائم المستحدثة سنة 2004 بموجب الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم:156/66 المتعلق بقانون العقوبات المعدل والمتمم بقسم سابع مكرر عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من:(394 مكرر – 394 مكرر 7). غير أن خطوته هذه تعتبر عملاقة في ذلك الوقت مقارنة بكثير من الدول التي تأخرت كثيرا في هذا المجال، مما مكّن أجهزة البحث والتحري من البدء في التعامل مع خصوصية هذا النوع من لجرائم المستحدثة واكتساب الخبرة مع مرور الوقت.

ثانيا: عدم كفاية وملاءمة النصوص القانونية: بالرغم من إصدار العديد من الدول للتشريعات المتعلقة بجرائم الإنترنت والحاسوب وانضمامها للعديد من الاتفاقيات الدولية التي تجرم الأفعال المخالفة للمعاهدات المنظمة لهذه الجرائم، إلا أن هذه النصوص غير كافية لمعالجة كافة أشكال الجرائم الإلكترونية، الأمر الذي يؤدي إلى تقليل جهود الأجهزة القضائية المكلفة بالبحث والتحري وبالتالي عدم القدرة على ضبط هذه الجرائم والكشف عن مرتكبيها.

كما أن كثيرا من التشريعات الداخلية للدول، وإن كانت تحتوي على قواعد عامة تحكم الجرائم التقليدية إلا أنه نظرا لاختلاف أركان وشروط الجرائم الإلكترونية مما يترتب عنه عدم إمكانية تطبيق هذه النصوص، مما يصعب مهمة أجهزة البحث والتحري في ملاحقة المجرم المعلوماتي[2].

وإدراكا من المشرع الجزائري بعدم كفاية النصوص القانونية لضمان مكافحة فعّالة لهذه الجرائم سواء على مستوى التجريم والعقاب أو على مستوى الإجراءات، وباعتبار أن تقنية المعلومات تنتشر في كافة أوجه الحياة اليومية وتتقدم بسرعة يوما بعد يوم وتتقدم معه أيضا أساليب المجرم المعلوماتي في ارتكاب جرائمه، لازال المشرع يقوم بتحديث المنظومة التشريعية المتعلقة بهذا المجال باستمرار

---

[1] عفيفي كامل عفيفي، المرجع السابق، ص467.

[2] نبيلة هبة هروال، المرجع السابق، ص63.

محاولا في ذلك مواكبة التطورات في مجال تكنولوجيات الإعلام والاتصال وكذا الاتجاه العالمي الموحد لمواجهة هذه الجرائم المستحدثة.

ثالثا: مشكلة اللغة المستخدمة للتحقيق والمحاكمة: تستخدم الثورة التكنولوجية في مجال تقنية المعلومات لغة علمية متخصصة تستخدم من طرف المبرمجين والعاملين في مجال صناعة الحوسبة. سميت هذه اللغة "بلغة المختصرات" *(Acronms)* يستخدمها خبراء الحاسوب للتواصل فيما بينهم. ومع بروز الجرائم الإلكترونية أصبحت هذه اللغة مهمة من حيث ضرورة معرفتها من طرف الجهات القضائية المختصة بالبحث والتحري وكذلك من قبل جهات المحاكمة، وتظهر أهمية ذلك أن الجريمة الإلكترونية تعتمد على التقنية المعلوماتية يُشار إليها برموز معروفة تكون الوسيلة الوحيدة للتخاطب بين مرتكبي هذه الجرائم والخبراء والمشغلين من جهة، وبين النيابة العامة والمحاكم من جهة أخرى[1].

ولتجاوز هذه العقبة يستلزم عقد دورات تدريبية لأعضاء النيابة العامة وقضاة التحقيق والحكم لاكتساب مهارات استعمال هذه اللغة بما يخدم الضبط والتحقيق والمحاكمة في ظل التطور المستمر لتقنية المعلومات والجرائم المرتبطة بها.

رابعا: نقص الخبرات لدى سلطات البحث والتحري: إن صعوبة اكتشاف الجريمة بالدرجة الأولي مرده إلى نقص خبرة المحققين مما يضعنا أمام معادلة غير متكافئة طرفها أجهزة التحقيق بنقص خبرتها في مجال الحاسوب والإنترنت، والطرف الآخر قراصنة يتمتعون بمهارات عالية يواكبون كل جديد في عالم المعلوماتية. وعليه تتعدد العوامل المساعدة في نقص الخبرة لدى جهات البحث والتحري في الكشف عن الجرائم الإلكترونية نذكر بعضها كما يلي[2]:

– ضعف الاعتمادات المالية المخصصة لسلطات البحث والتحري من أجل التكوين والتدريب والتأهيل الجيّد لمواجهة الجرائم الإلكترونية.

– حداثة الجريمة وخصوصيتها التي لم يعتد عليها المحققين، مما يجعلهم قاصرين في مواجهتها.

– ضخامة المعلومات والبيانات الموجودة على الإنترنت مما يصعب عملية البحث والتحري.

– البيئة الخصبة التي توفرها تكنولوجيات الإعلام والاتصال لارتكاب الجرائم الإلكترونية.

– انتشار الحاسوب على نطاق واسع وتعدد أنظمته وبرامجه وتطوره بشكل سريع.

---

1 أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت، المرجع السابق، ص295.

2 يوسف صغير، المذكرة السابقة، ص ص120-121.

وعليه يجب على السلطات القضائية العمل على ضرورة تنمية الخبرات والمهارات لأعضاء سلطة البحث والتحري في مجال تقنية المعلومات وشبكات الاتصال...إلخ، وذلك بوضع مناهج وبرامج مدروسة للتدريب على كيفية إثبات وضبط وملاحقة المجرم الإلكتروني في هذه البيئة الافتراضية، مراعين في ذلك خصوصية التطور التقني السريع دون إهمال للتعاون الدولي في هذا الشأن.

الفرع الثاني: الصعوبات الإجرائية:

قلنا سابقا أن ما يميز الجرائم الإلكترونية أنها ترتكب في مسرح إليكتروني أو مجال مفرغ يختلف كلياً عن المسرح التقليدي الذي ترتكب فيه الجريمة، حيث يتم الاستدلال عليها وضبطها وإثباتها بالوسائل التقليدية المتمثلة في إجراءات الاستدلال والتحقيق، فهي إجراءات صيغت لضبط وإثبات جرائم ترتكب في عالم مادي ملموس، يختلف تماما عن العالم الافتراضي. وهذا ما يشكل صعوبات إجرائية بالغة لأجهزة البحث والتحري تضاف إلى الصعوبات الموضوعية سالفة الذكر.

أولا: صعوبة إثبات هذه الجرائم: فالجرائم المعلوماتية تتميز بطبيعة خاصة وهذه الطبيعة تثير مشكلات كبيرة بخصوص إثبات الجرائم المعلوماتية والتي تتمثل في كون الحاسوب أداة الجريمة وأن الجريمة غالبا ما تعتمد في موضوعها على التشفير واستعمال الكود السري والأرقام والتخزين الإلكتروني، يصعب أن تخلّف وراءها آثارا مرئية قد تكشف عنها، أو يستدل من خلالها على الجناة ومثال ذلك: جرائم التجسّس المعلوماتي التي تتم بنسخ الملفات وسرقة وقت الآلة، يصعب على الشركات والمؤسسات التي تكون ضحية لها أن تكتشف أمرها وتلاحق مرتكبيها[1].

إن هذا التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات، يوضح لنا أن هذه النوعية من الجرائم لا تقع إلا من أشخاص لهم خبرة فنية كبيرة في مجال استخدام الحاسوب وشبكة الإنترنت ويتسمون بالذكاء الشديد، وأنهم يخططون جيدا لما يقومون به ويستخدمون قدراتهم الفنية والعقلية لإنجاح عملياتهم، لذا نجدهم يحيطون أنفسهم بتدابير أمنية وقائية تزيد من صعوبة كشفهم، ومن هذه التدابير استخدام جدران الحماية، كلمات السر والتشفير...إلخ[2].

---

[1] عادل عزام سقف الحيط، المرجع السابق، ص224.

[2] المرجع نفسه، ص194، راجع أيضا، عفيفي كامل عفيفي، المرجع السابق، ص469.

كما تتيح تقنية المعلومات إمكانية التخلص من هذه الأدلة الرقمية ومحوها[1]، أو صعوبة الوصول إليها باستعمال برامج التشفير التي تمكن المجرمين الإلكترونيين من تبادل المعلومات فيما بينهم بكل سرية وأمان[2]. ويتم ذلك عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح على اعتبار أنّ الجريمة تتم في صورة أوامر تصدر إلى الحاسوب، الأمر الذي يجعل كشف الجريمة وتحديد مرتكبها أمراً في غاية الصعوبة. ومع مرور الوقت اكتسب الجناة خبرة واسعة في التلاعب بالبيانات وإتلافها في غضون ثوانٍ معدودة قبل أن تتمكن الأجهزة المختصة من كشفهم أو التعرف عليهم، وذلك باستعمال ببرامج معينة لها خاصية إتلاف أو تدمير البيانات بصورة تلقائية بعد مضي فترة من الزمن بحسب رغبة مصمّم البرنامج وفي الوقت الذي يشاء[3] .

في هذا الشأن أيضا، يجتهد المهندسون في مجال تقنية المعلومات لابتكار برامج معينة لهذا الغرض، وتكمن آلية عملها في أنه بمجرد محاولة شخص غير مصرح له ولوج النظام أو استخدام جهاز الحاسوب المزود بهذا البرنامج ، فإن هذا الأخير يصدر أمراً للجهاز بحيث يتم إتلاف البيانات المخزنة به ومحوها بصورة تلقائية. ولعلّ صعوبة كشف الدليل تزداد بصورة خاصة متى ارتكبت هذه الجرائم في مجال العمل من قِبل العاملين ضد المؤسسات التابعين لها بحكم الثقة في هؤلاء، إذ يسهل عليهم اقتراف جرائمهم دون أن يتركوا أية آثار تدل عليهم[4].

من جهة أخرى، يجتهد الجناة في إخفاء هوياتهم للحيلولة دون تعقبهم أو كشف أمرهم ، بحيث تظل أنشطتهم مجهولة وبمنأى عن علم السلطات المعنية بمكافحة الجريمة مثل: استخدام الجاني حاسباً آخرا غير حاسبه الشخصي الموجودة بالأماكن العامة، أو اللّجوء إلى مقاهي الإنترنت، على اعتبار أن جل هذه المقاهي لا تقوم بتسجيل أسماء مرتاديها أو التحقّق من هوياتهم، لاسيما إذا علمنا أن شبكة الإنترنت تتيح لمستخدميها استعمال الخط الواحد لأكثر من شخص وفي وقت واحد معا ، ما يجعل المراقبة والتعقب للمشتبه فيه أمراً ينطوي على صعوبة وغير ميسور في كثير من الأحيان وربّما تتعقد المسألة أكثر عند استخدام الإنترنت اللاّسلكي[5].

---

[1] حيث قام شخص من ألمانيا بإدخال في نظام الحاسوب تعليمات أمنية لحماية البيانات المخزنة فيه من المحاولات الرامية للوصول إليها من شأنها محو هذه البيانات بواسطة مجال كهربائي، وذلك إذا ما تم اختراقه من قبل شخص غير مرخص له، راجع، فؤاد حسين العزيزي المرجع السابق، ص192.

[2] *Mohammed Buzubar, art-Cit,p.71.*

[3] موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية ، المؤتمر المغاربي الأول حول :المعلوماتية والقانون، أكاديمية الدراسات العليا ، يومي: 28 و29 أكتوبر 2009، طرابلس، ليبيا، ص3.

[4] المرجع نفسه، ص3.

[5] هلالي عبد الإله أحمد، الجوانب الموضوعية، المرجع السابق، ص160، راجع أيضا، يوسف صغير، المذكرة السابقة، ص ص118-119.

من جانب آخر، تقتضي الخصائص العامة للجريمة الإلكترونية، أن تكون جهات البحث والتحري على درجة كبيرة من المعرفة بأنظمة الحاسوب وكيفية تشغلها، وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها وضبط الأدوات التي استخدمت في ارتكابها والتحفظ على البيانات أو الأجهزة التي استخدمت في ارتكابها أو تلك التي تكون محلا للجريمة. مما يتطلب من المحقّق أن تكون لديه دراية علمية كافية ومتابعة مستمرة لكل ما هو جديد في مجال تقنية المعلومات[1].

ثانيا: صعوبة درء واكتشاف تلك الجرائم: لا تحتاج الجرائم الإلكترونية إلى أي عنف، أو سفك للدماء، أو أثار اقتحام لسرقة الأموال، وإنما هي أرقام وبيانات في شكل نبضات إلكترونية يمكن محوها أو تعديلها أو تغييرها تماما من السجلات المخزونة في ذاكرة الحاسوب، ولأن هذه الجرائم في أغلب الأحيان لا تترك أي أثر خارجي مرئي لها فإنها تكون صعبة في الإثبات. ومما يزيد من صعوبة إثبات هذه الجرائم أيضاً ارتكابها عادة في الخفاء، وعدم وجود أي أثر كتابي لما يجرى خلال تنفيذها من عمليات أو أفعال إجرامية، حيث يتم نقل البيانات بواسطة النبضات الإلكترونية، إضافة إلى إحاطة شبكات الاتصال بجدار من الحماية الفنية بقصد إعاقة محاولة الوصول غير المشروعة إليها كاستخدام كلمات السر أو تقنيات التشفير[2].

من جانب آخر يلعب مجتمع الأعمال دورا سلبيا في عدم الإبلاغ عن الجرائم المعلوماتية، إذ تحرص الشركات والمؤسسات الاقتصادية التي تتعرض أنظمتها المعلوماتية للانتهاك أو القرصنة لخسائر مادية فادحة ولا تكشف عن ذلك حتى لموظفيها، وتكتفي باتخاذ إجراءات داخلية دون إبلاغ السلطات القضائية المختصة، وهذا تجنبا للإضرار بسمعتها واهتزاز الثقة أمام زبائنها[3].

وعليه غالبا ما تكتشف الجرائم الإلكترونية بمحض الصدفة، فمثلا: جريمة التجسّس المعلوماتي بنسخ الملفات وسرقة وقت الآلة من النادر اكتشافها من طرف الشركات التي تقع ضحية لها وما يزيد من صعوبة الأمر أن الجريمة تتم عن بعد، ومن ثمة تتباعد المسافات بين الفعل والنتيجة[4] .

ثالثا: صعوبة ملاحقة المجرم الإلكتروني: لا يتعلق الأمر هنا بملاحقة المجرم التقليدي، فسارق جهاز الحاسوب أو من يقوم بإتلاف وحداته الإلكترونية بشكل يدوي يمكن لأجهزة البحث والتحري

---

[1] عفيفي كامل عفيفي، المرجع السابق، ص470.

[2] فؤاد حسن العزيزي، المرجع السابق، ص ص192-193، راجع أيضا، أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت المرجع السابق، ص290.

[3] حنان ريحان مبارك المضحكي، المرجع السابق، ص39.

[4] عفيفي كامل عفيفي، المرجع السابق، ص470.

ملاحقته والقبض عليه بسهولة، لكننا نتحدث عن الجريمة الإلكترونية أين يقوم الجاني بسرقة المعطيات أو التلاعب فيها أو استغلالها أو تخريب الأنظمة المعلوماتية، وذلك باستعمال تقنيات المعلوماتية نفسها، وهو جالس في بيته وبضغطة زر[1].

إن ملاحقة بالمجرم الإلكتروني لهو من الصعوبة بمكان، حيث يتطلب إثبات التهمة عليه فحص أجهزته الإلكترونية واقتحام أسراره التكنولوجية لاستخلاص الدليل الرقمي المفضي لإدانته، وما يثير ذلك من صعوبات تقنية بالغة لأجهزة البحث والتحري، ناهيك عن خصوصية هذا النوع المستحدث من الجرائم، فهي جرائم عابرة للحدود يمكن أن يتوزع ارتكاب الركن المادي للجريمة على مجموعة من الأشخاص ينتمون لدول مختلفة، وما ينتج عن ذلك من مشكلات متعلقة بتنازع الاختصاص، لذا اتجهت معظم الدول للتنسيق فيما بينها في مجال التعاون القضائي والمساعدة القضائية الدولية مثل: تنفيذ طلبات المساعدة القضائية الدولية وتسليم المجرمين...إلخ.

رابعا: صعوبات متعلقة بالمساعدة القضائية الدولية: تتميز الجرائم الإلكترونية بأنها جرائم عابرة للحدود نتيجة استعمال شبكة الإنترنت، فإذا ارتكبت الجريمة عبر الإنترنت تزداد العقبات القانونية صعوبة، فلا نكون أمام مشكلات إجرائية تخص ضبط الجريمة وإثباتها فحسب، بل نجد أنفسنا أمام مشكلة أكثر تعقيداً تتمثل في تحديد الاختصاص القضائي المرتبط بتحديد القانون الواجب التطبيق على هذه الجريمة، على اعتبار أن قواعد الاختصاص القضائي التقليدية صيغت لكي تحدد الاختصاص المتعلق بجرائم قابلة للتحديد المكاني للجريمة، وهي قواعد ترتكز على مبدإ الإقليمية وهو ما يرتبط بسيادة الدولة، فلا يكون الخروج عليه بقبول اختصاص قضائي أجنبي إلا في حالات استثنائية يجب النص عليها صراحة. وعليه تُثار مسألة مدى امكانية الاعتماد على هذه القواعد لتحديد الاختصاص القضائي لجريمة ترتكب في مجال تنعدم فيه الحدود الجغرافية، وكثيرا ما يكون مرتكبوها في دول مختلفة ومن جنسيات متعددة، إضافة إلى توزع السلوك الإجرامي والنتيجة على أكثر من دولة[2].

وعليه تعتبر المساعدة القضائية الدولية بمختلف صورها كالإنابة القضائية وتبادل المعلومات وتسليم المجرمين...إلخ، من أهم صور التعاون الدولي في المجال الجنائي، غير أنها تتم بالطرق الدبلوماسية مما يجعلها تتسم بالبطء والتعقيد، والذي يتعارض مع طبيعة الجرائم الإلكترونية التي تتميز بالسرعة العالية في التنفيذ، إضافة إلى مشكل التماطل في الرد على طلبات المساعدة القضائية وتقييدها بشروط معينة، أو بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللّغوية أو الفوارق في

---

[1] ناير نبيل عمر، المرجع السابق، ص164.

[2] يوسف المصري، المرجع السابق، ص131.

طبيعة الإجراءات بين الدول والتي تُعقّد الاستجابة في الوقت المناسب مما يتيح الفرصة لإفلات المجرم المعلوماتي وفقدان آثاره في هذه البيئة الافتراضية[1].

خامسا: صعوبات متعلقة بالتعاون الدولي في مجال التدريب: رغم أهمية عملية تدريب أعضاء الأجهزة القضائية في مجال البحث والتحري عن الجرائم الإلكترونية للكشف عنها وملاحقة مرتكبيها، إلا أن هناك بعض الصعوبات المعترضة نوجزها فيما يأتي[2]:

– عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون.

– وُجود فوارق فردية بين المتدربين وتأثيرها على عملية اكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الأفراد المتدربين، لاسيما في مجال تقنية المعلومات وشبكات الاتصال.

– النظرة السلبية للمتدرب اتجاه العملية التدريبية على أنها عبء لا طائل منه، مما ينتج عنه عدم تجديد للمعارف والخبرات خاصة في مجال مكافحة الجرائم الإلكترونية.

– عدم قدرة البيئة التدريبية على تمثيل الواقع العملي لبيئة العمل الطبيعية تمثيلا تاما ومتقنا، من حيث ما يدور بها من وقائع وملابسات وإجراءات لا تبلغ حد التطابق مع طبيعة المهام التي سيقوم بها المتدربون، خاصة أنها تتم في وسط افتراضي.

– ارتفاع كلفة الدورات التدريبية مما لا يتيح لكثير من الدول تمكين أفراد أجهزتها القضائية الاستفادة منها.

ورغم هذه الصعوبات، اهتمت الكثير من الدول المتقدمة بتدريب المحققين في الجرائم الإلكترونية حيث دعا المجلس الأوروبي في إحدى توصياته سنة 1999 إلى ضرورة تدريب الشرطة وأجهزة العدالة بما يواكب التطور المتلاحق لتقنية المعلومات واستخدامها لتحقيق التوازن بين وسائل ارتكاب الجريمة وبين سبل مواجهتها، وعقدت كذلك المنظمة الدولية للشرطة الدولية العديد من الدورات التدريبية لمحققي جرائم الحاسب الآلي[3]. وإدراكا من الجزائر بأهمية مكافحة هذه النوع المستحدث من الجرائم تقوم

---

1 حسين بن سعيد الغافري، السياسة الجنائية، المرجع السابق، ص694.

2 يوسف المصري، المرجع السابق، ص ص131-132.

3 موسى مسعود أرحومة، المرجع السابق، ص5.

مختلف الأسلاك الوطنية كالمديرية العامة للأمن الوطني[1] والدرك الوطني[2] بعقد ملتقيات وطنية ودولية ودورات تدريبية ذات الصلة لتأهيل أعضاء أجهزة البحث والتحري في مجال تأمين الفضاء السبراني ومكافحة الجريمة الإلكترونية. حيث يتطلب كشف هذه الجرائم أن تكون الأجهزة المعنية على دراية كافية بأساسيات التعامل مع هذه الجرائم وكيفية تقصّيها وضبطها وصولاً إلى مرتكبيها، ما يعني ضرورة تلقّي هؤلاء دورات تدريبية بشأن استراتيجية التحقيق والاستدلال عن هذه الجرائم.

[1] في هذا الشأن، عقدت بالجزائر بمدينة وهران بتاريخ:2013/09/10، أشغال الدورة الـ22 للندوة الإقليمية الإفريقية للمنظمة الدولية للشرطة الجنائية *(Interpol)* بمشاركة 53 بلدا، لبحث الواقع الراهن والمستقبلي وآليات مكافحة الأشكال الجديدة والمتجددة للجريمة المنظمة والعابرة للحدود، ومنها الجرائم الإلكترونية، حيث يتطلب الأمر تحيين المعارف والمعلومات لمواجهتها عن طريق تعزيز التعاون الجهوي والدولي من خلال تبادل المعلومات والخبرات والتجارب وعقد الدورات، لأكثر تفاصيل، يرجى زيارة الموقع الرسمي للمديرية العامة للأمن الوطني على الرابط الآتي:

http://www.dgsn.dz/?%D8%A7%D9%81%D8%AA%D8%AA%D8%A7%D8%AD-%D8%A3%D8%B4%D8%BA%D8%A7%D9%84,2439 ، تاريخ الاطلاع:2016/08/22 على الساعة:06:35.

[2] في هذا الصدد نظمت قيادة الدرك الوطني، الندوة الدولية حول: "الأمن السيبراني بالجزائر"، وذلك يومي 24 و25 ماي 2016 بالنادي الوطني للجيش "ببني مسوس" بالجزائر العاصمة، بمشاركة وفود أجنبية وخبراء وطنيين ودوليين من 15 دولة ذوي مستوى عالي في مجال الأمن السبراني. حيث ستعالج هذه الندوة حالة التطور التكنولوجي والتشريعات في الفضاء السيبراني، من خلال عدة محاور شملت: "الفضاء السبراني كبعد جديد للأمن الوطني"، "السياسات الوطنية للأمن السبراني"، "التشريعات والفضاء السبراني"، "الوقاية من جرائم الإنترنت ومكافحتها"، "أمن المنشآت الحساسة"، "الخدمات الالكترونية والأمن الرقمي"، "الأمن السبراني من خلال البحث والتطوير". كما شمل الملتقى الدولي على ورشات عمل وتمارين محاكاة التي تنظم بالاشتراك مع الخبراء الوطنيين والدوليين لتعزيز قدرات أجهزة البحث== ==والتحري في مجال مكافحة الأشكال الجديدة للجريمة الرقمية، أكثر تفاصيل يرجى زيارة الموقع الرسمي لقيادة الدرك الوطني على الرابط الآتي:*http://www.mdn.dz/site_principal/index.php?L=ar#undefined* ، تاريخ الاطلاع:2016/08/22 على الساعة:06:49.

خلاصة الفصل الثاني:

تطرقنا في هذا الفصل إلى مجمل القواعد الوقائية التي نص عليها المشرع الجزائري في سياسته الجنائية الإجرائية، والتي تهدف إلى الكشف المبكر للاعتداءات المحتملة لمرتكبي الجرائم الإلكترونية إضافة إلى النص على إجراء التعاون والمساعدة القضائية الدولية في مجال مكافحة الجرائم الإلكترونية. حيث نص على مراقبة الاتصالات الإلكترونية وشروطها وحالات اللجوء إليها، والتي تتم بأي وسيلة إلكترونية بموجب المادة(03) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث ميّز المشرع بين المعطيات المتعلقة بالمحتوى بموجب المادة (04)، والمعطيات المتعلقة بحركة السير بموجب المادة(11) مع وجهة نظر مزدوجة للشروط القانونية الواجب توافرها من أجل الإذن بكل إجراء تماشيا مع الاتفاقيات الدولية في هذا الشأن، إضافة إلى تحديد حالات اللّجوء إلى هذا الإجراء بموجب المادة (04) وربط ذلك بوجود ضرورة قصوى إعمالا لحق الأشخاص في الخصوصية المحمي دستوريا.

من جهة أخرى، ونظرا لأهمية الدور الفعّال الذي يلعبه مقدمو الخدمات في مكافحة الجرائم الإلكترونية عن طريق تسهيل الوصول إلى الأدلة الرقمية، رأى المشرع أنه من الضروري إلزام الأطراف المتدخلة في توفير الخدمات، بتقديم المساعدات الضرورية للجهات القضائية المكلفة بالتحريات والتحقيقات وعليه نص المشرع بموجب المادتين (11-10) من القانون رقم: 09-04 سالف الذكر على الالتزامات الملقاة على عاتقهم، والمتمثلة في مساعدة السلطات القضائية وحفظ المعطيات المتعلقة بحركة السير وذلك تحت طائلة العقوبات الإدارية والجزائية في حالة الإخلال بها. وفي الشأن نفسه، فرض المشرع أيضا التزامات على عاتق مزودي خدمة الإنترنت، بموجب المادتين (11-12) من القانون رقم: 09-04 إضافة إلى المادة (14) من المرسوم رقم: رقم:98-257 المؤرخ في:1998/08/25 يضبط شروط وكيفيات إقامة خدمات انترنات واستغلالها. ينجّر عنها تحمّل مسؤوليتهم سواء كانوا أشخاصا طبيعيين أو معنويين في حالة الإخلال بها، وذلك نظرا لحساسية هذا القطاع بالنسبة للدولة والمواطن على حد سواء، وما يشكله أيضا من بيئة خصبة لانتشار الجرائم الإلكترونية.

من جانب آخر وبسبب الطبيعة الخاصة للجريمة الإلكترونية وخطورتها، أجاز المشرع الدخول بغرض التفتيش ولو عن بعد إلى المنظومة المعلوماتية ودون إذن صاحبها، وكذا حجز المعطيات بموجب المادتين (05) و(06) من القانون 09-04 سالف الذكر، إضافة إلى تمديد هذا الإجراء إلى كافة الإقليم الوطني، حيث جعل من إجراء التفتيش وحجز المعطيات مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة الإلكترونية. كما حدد المشرع بوضوح الجهة القضائية المختصة سواء في مجال

الإذن بوضع ترتيبات للمراقبة الإلكترونية للحيلولة دون الاعتداء على منظومة معلوماتية، أو في مجال الدخول بغرض التفتيش ولو عن بُعد لمنظومة معلوماتية أو جزء منها أو منظومة تخزين معلوماتية سواء تقع داخل الاقليم الوطني أو خارجه.

من جهة أخرى لم تتوقف السياسة الجنائية الإجرائية للمشرع الجزائري بخصوص مكافحة الجرائم الإلكترونية داخل الوطن، وإنما امتدت خارجه في إطار التزاماته الدولية لتشمل التعاون الدولي وطلبات المساعدة القضائية تنفيذا للتوصيات الدولية بضرورة تظافر جهود الدول لمكافحة هذا النوع من الجرائم، فنص بموجب المادة (15) من القانون رقم:09-04 على تمديد اختصاص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني. كما نص في المادة (16) من القانون نفسه على تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني وأيضا شروط قبولها بموجب المادة (17)، كما فرض قيودا على طلبات المساعدة القضائية تماشيا مع احترام مقتضيات النظام العام ومبدأ سيادة الدولة على إقليمها. وفي الأخير تناولنا بعض الصعوبات الموضوعية والإجرائية التي تواجهها سلطات البحث والتحري باعتبارها الواجهة الأولى في الكشف عن الجريمة الإلكترونية ومرتكبيها.

الخاتمة

تناولنا في هذه الدراسة الجوانب الموضوعية والإجرائية، التي أقرّها المشرّع الجزائري في إطار مكافحة الجرائم الإلكترونية بمفهومها الواسع، سواء التي تتم بواسطة الحاسوب عندما يكون وسيلة لها أو تلك التي تقع على الحاسوب عندما يكون هدفا لها، أو تلك التي تتم بواسطة أية وسيلة إلكترونية وعموما من خلال تكنولوجيات الإعلام والاتصال. وباعتبار الجرائم الالكترونية جرائم مستحدثة تعدّدت المفاهيم والتعريفات الدالة عليها، حيث أخذ المشرع بالمفهوم الموسّع للجرائم الإلكترونية –وهو مسلك محمود–التي ترتكب بوسائل متعددة، كاستعمال الحاسوب وشبكة الإنترنت والهاتف النقّال واللاّسلكي، وأية وسيلة إلكترونية أو معلوماتية تظهر في المستقبل، وبالتاليساير المشرع التطورات المذهلة الحاصلة في مجال الحوسبة والاتصالات. يظهر ذلك جليا من خلال استعمال المشرّع لمصطلح" الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" للدلالة على الجرائم الإلكترونية فهو يزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة.

من جانب آخر، وفّرت التكنولوجيا الحديثة سهولة اتصال الحاسوب أو الهاتف النقال بشبكة الإنترنت، التي تقدم خدمات لا تحصى في شتى المجالات، كالتواصل بين الأفراد وتبادل المعلومات ومعالجة البيانات والتجارة الإلكترونية وبنوك الإنترنت واستعمال وسائل الدفع الإلكتروني...إلخ. مما نتج عنه تعدد أشكال الجريمة الإلكترونية، التي تستوجب الدراسة الدقيقة للبنيان القانوني لها، حيث تناولنا أركانها إضافة إلى توضيح إشكالية مدى اعتبار المعلوماتية موضوعا لنصوص جرائم الأموال ومدى خضوعها أيضا لنصوص الملكية الصناعية والأدبية، وخلصنا إلى إضفاء المشرّع الحماية الجزائية على برامج الحاسوب وقواعد البيانات باعتبارهما قيما مالية مستحدثة، وهذا بموجب الأمر رقم:03-05 المؤرخ في: 2003/07/19 يتعلق بحقوق المؤلف والحقوق المجاورة.

أما على صعيد التجريم والعقاب، قام المشرع الجزائري بخطوة أولى تمثّلت في النصّ على تجريم الاعتداءات على شرف واعتبار الأشخاص وعلى حياتهم الخاصة باستعمال تكنولوجيات الإعلام والاتصال، مثل: جرائم الإهانة أو السب أو القذف باستعمال الوسائل الإلكترونية أو المعلوماتية وعموما بأي وسيلة إلكترونية توفّرها التقنية الحديثة بموجب المواد:(144مكرر) و(144مكرر2) و(146) من قانون العقوبات. وفي الاتجاه نفسه، نصّت المواد (303مكرر–303مكرر3) من قانون العقوبات على جرائم المساس بحرمة الحياة الخاصة للأفراد باستعمال الوسائل التقنية.

وفي الشأن ذاته، ونظرا لخطورة الجرائم الإلكترونية، قام المشرع بخطوة ثانية مهمة في سياسته الجنائية الرامية لمواجهتها، تمثّلت في تعديل قانون العقوبات مرة أخرى بموجب القانون رقم:04-15 المؤرخ في:10 نوفمبر2004، بإضافة قسم سابع مكرر عنوانه:" جرائم المساس بأنظمة المعالجة

الآلية للمعطيات" من المواد(394 مكرر إلى 394مكرر7) مثل: جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات وجريمة التلاعب في معطيات نظام المعالجة الآلية للمعطيات وغيرها. كما اتجه المشرع إلى تجريم بعض أشكال الجرائم الإلكترونية بموجب بعض القوانين الخاصة كقانون البريد والمواصلات السّلكية واللاّسلكية، وقانون التأمينات الاجتماعية الذي نصّ على الجرائم المتعلقة بإساءة استخدام بطاقة الضمان الاجتماعي. إضافة إلى النصّ على الجرائم الخاصة بالتوقيع والتصديق الإلكترونيين بموجب القانون رقم:15-04 المؤرخ في:2015/02/01 يتعلق بالتوقيع والتصديق الإلكترونيين.

غير أننا نسجّل عدم نص المشرّع على بعض الجرائم رغم أهميتها، مثل: جريمة التزوير المعلوماتي، جرائم إفساد النظام المعلوماتي، جريمة الترويج والاتجار بالمخدرات الرقمية، وعليه يجب على المشرع تدارك هذا الفراغ التشريعي من خلال تعديل النصوص التقليدية، أو استحداث نصوص أخرى جديدة تتلاءم وطبيعة هذه الجرائم.

وباعتبار الجرائم الإلكترونية، جرائم عابرة للحدود يتطلب مكافحتها تظافر جهود الدول، قام المشرّع الجزائري بالتصديق على نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، إضافة إلى إبرام اتفاقيات ثنائية بخصوص التعاون القضائي والمساعدة القضائية الدولية، والتي تعتبر خطوات هامة على صعيد المكافحة الدولية لهذه الجرائم.

أما فيما يتعلق بالجانب الإجرائي، فلقد تطرقنا إلى بعض الإجراءات التقليدية كإجراء المعاينة والخبرة ومدى انطباق هذه الإجراءات على الجرائم الإلكترونية، حيث تبين أنّها غير كافية ولا تتلاءم مع طبيعتها، مما دفع بالمشرّع إلى تعديل قانون الإجراءات الجزائية بموجب القانون رقم:06-22 المؤرخ في 2006/12/20 المعدل والمتمم، أين استحدث أساليب خاصة للبحث والتحرّي عن بعض الجرائم على سبيل الحصر، ومنها الجرائم الإلكترونية، مل: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرّب، وذلك بموجب المواد من (65 مكرر5 - 65 مكرر18).

وبهدف تسهيل مهام أجهزة البحث والتحرّي في إطار مكافحة هذا النوع المستحدث من الجرائم سارع المشرّع إلى تمديد الاختصاص القضائي لبعض المحاكم بموجب المرسوم التنفيذي رقم:06-348 المؤرخ في:2006/10/05، إضافة إلى وكلاء الجمهورية بموجب المادة(2/37) وقضاة التحقيق بموجب المادة(2/40). من جانب آخر، قام بتمديد الاختصاصات المكانية للضبطية القضائية بموجب المادة(7/16)، على اعتبار أنها الواجهة الأولى في الكشف عن الجريمة وملاحقة المجرم الإلكتروني. كما وسّع أيضا من الاختصاص المحلي للنيابة العامة في مجال تتبع الجرائم

الإلكترونية، وأجبرها بأن تباشر إجراءات المتابعة الجزائية تلقائيا، وذلك في المواد(144 مكرر-144 مكرر2) من (ق.ع.ج) والمتعلقة بجرائم القذف باستعمال أيّ وسيلة إلكترونية أو معلوماتية.

غير أنّ المشرّع الجزائري لم يكتف بهذا التعديل رغم أهميته البالغة، بل اتّجه إلى إقرار سياسة جزائية وقائية من الجرائم الإلكترونية، وذلك بموجب القانون رقم: 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أين نصّ على جملة من الإجراءات الخاصة، مثل: تفتيش المنظومة المعلوماتية داخل الإقليم الوطني أو خارجه، وحجز المعطيات المعلوماتية والتعاون القضائي والمساعدة الدولية المتبادلة.

بناء على ما سبق ذكره، خلصنا في دراستنا هذه إلى ما يأتي:

أولا: النتائج: نوجزها كما يلي:

- نظرا للطبيعة الخاصة للجريمة الالكترونية، لا يوجد اتفاق على وضع تعريف موحد لها، أو استعمال مصطلح معيّن للدلالة على هذه الظاهرة الجرمية الناشئة في بيئة الكمبيوتر والإنترنت، وهو اختلاف رافق ظاهرة الإجرام المرتبط بتكنولوجيات الإعلام والاتصال، فهي تتم في فضاء افتراضي يتسم بالتغيير والانتشار الجغرافي العابر للحدود. كما انعكس ذلك أيضا عند محاولة وضع تصنيف لها، فتبين أنّها ليست صنفا واحدا وبالتالي تعددت التصنيفات، سواء ما تعلق بمحل الجريمة أو دور الكمبيوتر في ارتكابها، أو كجرائم ماسة بالأموال أو الأشخاص أو جرائم انترنت، واختلفت باختلاف أنواع الجرائم الإلكترونية، مما يخلق صعوبات جمّة في مكافحتها سواء على المستويين الموضوعي أو الإجرائي.

- اتضح لنا من خلال دراستنا أنّ النصوص القانونية التقليدية، سواء الموضوعية منها أو الإجرائية لا تكفي لمواجهة هذه الجرائم المستحدثة بسبب طبيعتها الخاصة، وهذا ما أدركه المشرّع الجزائري فسارع إلى تعديل منظومته التشريعية بدءا من سنة 2004 -رغم أنه كان متأخرا بعض الشيء عن كثير من الدول التي سبقته في هذا المجال-إلاّ أنّ هذه الخطوة كانت الأساس في مكافحة الجرائم الإلكترونية.

- لقد اعتمد المشرع الجزائري مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" وعرّفها بموجب أحكام المادة (02/أ) من القانون رقم:04 -09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وعليه وُفّق المشرع الجزائري في اختياره

لهذا المصطلح للدلالة على هذه الجرائم المستحدثة، والذي يتوافق أيضا مع مصطلح "الجرائم الإلكترونية" بالمفهوم الواسع والمستعمل في بحثنا.

- كما تتميز الجرائم الإلكترونية بخصائص متفردة عن باقي الجرائم، سواء ما تعلق بالمجرم الإلكتروني كالذكاء والاحترافية، أو بأنواع المجنى عليهم، أو بمراحل ارتكابها أو ما تعلق بالجريمة نفسها، فهي جرائم عابرة للحدود ويصعب على المحقّقين اكتشافها وإثباتها، وتتم بأساليب وأدوات متنوعة، يغلب عليها الطابعان التقني والفني وهذا ما يميزها عن باقي الجرائم التقليدية.

- تتسبب الجرائم الإلكترونية في أضرار نفسية واجتماعية واقتصادية بالغة يصعب حصرها وبالتالي كان لزاما على المشرّع عند وضعه لسياسته الجنائية، الإحاطة الشاملة والمعرفة الدقيقة بماهيتها وبكافة صورها، وتحديد أركانها وأوجه النشاط الجرمي فيها، قصد تحقيق الفعالية في مكافحتها وضمان عدم إفلات المجرم.

- استعمل المشرع مصطلح" منظومة " بدلا من مصطلح "نظام" لترك الباب مفتوحا في حال ظهور منظومات معلوماتية جديدة مع تعدد استعمالاتها.

- أضفى المشرّع الحماية الجزائية على برامج الحاسوب وقواعد البيانات بموجب الأمر رقم:03-05 يتعلق بحقوق المؤلف والحقوق المجاورة، بهدف حمايتها من جرائم التقليد.

- لم يشترط المشرع لقيام الجريمة الإلكترونية خضوع النظام المعلوماتي للحماية الفنية، حيث يهدف المشرع من وراء ذلك إلى إضفاء الحماية الجزائية على كافة أنظمة المعالجة الآلية للمعطيات بغض النظر عن تمتعها بالحماية الفنية أم لا.

- التوسّع في مفهوم الدخول غير المشروع، ليشمل فعلي الدخول والبقاء، وتجريم أفعال التلاعب في معطيات المنظومة المعلوماتية مثل: إدخال أو إزالة أو تعديل معطيات المنظومة، ما لم يكن مصرحا بذلك. وهذا بقصد ضمان سريتها وسلامتها ووفرتها.

- وسّع المشرع من نطاق الحماية لتشمل كافة أنواع المعلومات وجميع وسائل التلاعب بها كأفعال الاعتداء على سلامة المعطيات خارج المنظومة المعلوماتية عن طريق الحيازة والإفشاء...إلخ.

- حصر السلوك المجرّم في جريمة التعامل في معلومات غير مشروعة في المعطيات المخزنة أو المعالجة أو المرسلة فقط بواسطة منظومة معلوماتية، في حين تتوسّع في ذلك بعض التشريعات المقارنة، ومنها التشريع الفرنسي.

- مضاعفة العقوبة تبعا لصفة المجنى عليه، وذلك إذا مسّت هذه الجرائم الدفاع الوطني أو الهيآت والمؤسسات الخاضعة للقانون العام، وهو مسلك حسن انفرد به المشرع الجزائري.

– تبني المشرع مبدأ مسؤولية الشخص المعنوي الذي يرتكب هذه الجرائم وشدّد من العقوبة عليها.

– وسّع المشرع من نطاق العقوبة، وذلك بتجريم الشروع والاتفاق الجنائي، والنصّ على العقوبات التكميلية كالمصادرة والغلق، وهو اتجاه محمود من المشرع لإضفاء فكرة الردع العام والخاص بخصوص هذا النوع المستحدث من الجرائم.

– وقّر المشرع قدرا من الحماية الفنية والجزائية لوسائل الدفع الإلكتروني، رغم أن استعمالها قليل في الجزائر، وذلك من خلال قانون البريد والمواصلات السلكية واللاسلكية رقم: 2000–03المؤرخ في:2000/08/05 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السّلكية واللاّسلكية أين نصّ المشرع على تجريم الأفعال الماسة بسرّية ومضمون المراسلات بواسطة اللاّسلكي. كما نصّ أيضا على جرائم إساءة استخدام البطاقة الإلكترونية للضمان الاجتماعي بموجب القانون رقم:08–01 المؤرخ في:2008/01/23 يتعلق بالتأمينات الاجتماعية، تماشيا مع توجهات المشرع الداعية الى استعمال الوسائل الإلكترونية في عمليات الدفع الإلكتروني، كما نص على الجرائم المتعلقة بالتوقيع والتصديق الإلكترونيين بموجب القانون رقم:15–04 المؤرخ في:2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

– ألزم المشرّع الأطراف المتدخلة في توفير الخدمات ومنها خدمات الإنترنت، سواء كانوا أشخاصا طبيعيين أو معنويين بتقديم المساعدات الضرورية للجهات القضائية المكلفة بالتحريات والتحقيقات، وكذا حفظ المعطيات المتعلقة بحركة السير، وذلك تحت طائلة العقوبات الإدارية والجزائية وهو ما يساعد على توفير مكافحة جزائية فعّالة لهذه الجرائم.

– لم ينص المشرع الجزائري على جريمة التزوير المعلوماتي، برغم ما تمثّله من خطورة على المصالح المحمية قانونا.

– لم يجرّم المشرّع الجزائري كافة أشكال الإرهاب الإلكتروني، الذي أصبح لا يستغنى عن استعمال تقنية المعلومات، حيث اقتصر المشرع على جريمة الإشادة بالأفعال الإرهابية، التي تتم بأية وسيلة كانت.

– تعزيز السياسة الجنائية للمشرع الجزائري في هذا المجال، بالتصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، حيث أقرّت عددا من الجرائم لم ينص عليها المشرع بعدُ مثل: جريمة الاعتراض غير المشروع للبيانات وجريمة الإباحية الإلكترونية والتزوير المعلوماتي وترويج وتجارة

المخدرات عبر شبكة الإنترنت، والإرهاب الإلكتروني، ونأمل أن يستدرك ذلك في أقرب الآجال بتحويل نصوص الاتفاقية إلى نصوص تشريعية، قياسا بسرعة تطور وانتشار تقنية المعلومات.

– نظرا لعدم كفاية الإجراءات التقليدية المتعلقة بالبحث والتحرّي عن الجرائم الإلكترونية، سارع المشرّع إلى استحداث أساليب خاصة بموجب المادة (65 مكرر5 – 65 مكرر18) من قانون الإجراءات الجزائية، يهدف من وراء ذلك إلى استخلاص الدليل الرقمي، الذي تختلف طبيعته عن الدليل التقليدي.

– أقرّ المشرّع الإثبات بالكتابة في شكلها الإلكتروني وبصحة التوقيع الإلكتروني وتساويه في الحجية مع التوقيع الفيزيائي، والتخلي عن ما يحُدُ من الإثبات في البيئة التقنية، تماشيا مع الاتجاه العالمي السائر نحو الاعتراف التام بحجية الأدلة الرقمية في مجال الإثبات الجنائي. وهذا ما جسّده في جملة من النصوص، مثل: الإثبات بالكتابة في الشكل الإلكتروني بخصوص المعاملات المدنية(المادة 323 مكرر1) من القانون المدني، إضافة إلى نص المادة (1/02) من القانون رقم:15-04 المؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

– نصّ المشرّع على إجراءات وقائية بموجب القانون رقم: 09-04 المؤرخ في: 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الهدف منها الوقاية من الجريمة الإلكترونية قبل حدوثها، مثل: مراقبة الاتصالات الإلكترونية وتفتيش المنظومة المعلوماتية وحجز المعطيات، والتعاون القضائي والمساعدة الدولية المتبادلة وفق شروط معينة.

-التوسّع في محلّ الحماية ليشمل فعل الدخول والبقاء غير المشروعين في كل المنظومة المعلوماتية أو جزء منها.

– لم يجرّم المشرّع الجزائري جريمة إفساد سير نظم المعالجة الآلية للمعطيات واكتفى بنصوص المواد (394 مكرر الى 394 مكرر2) والمتمثلة في فعل اعتراض والتقاط المراسلات، التي تتم داخل النظام المعلوماتي أو بين مجموعة من الأنظمة، في حين جرّمته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب المادة(7)، وجرمته أيضا المادة (3) من الاتفاقية الأوروبية للإجرام المعلوماتي. حيث يطرح التساؤل عن عدم إفراد المشرّع لنصّ خاص لتجريم هذه الأفعال، وخاصة أنّها جرائم أساسية ترتكب ضد الأنظمة المعلوماتية؟، إذ لا يعتبر نص المادة (394 مكرر) كافيا لذلك.

- لم يجرّم المشرّع الجزائري سرقة وقت الآلة، وإنما جرّم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، ربما اعتقاد منه بأن الحماية الجنائية للمعطيات، هي حماية غير مباشرة للنظام المعلوماتي بموجب المادة(394 مكرر).

- يلاحظ تأثر المشرّع الجزائري أثناء وضع سياسته الجنائية بشقيّها الموضوعي والإجرائي في مكافحة الجرائم الإلكترونية بنظيره الفرنسي، وكذا بالاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي.

ثانيا: التوصيات: بناء على ما سبق ذكره، نخلص إلى التوصيات الآتية:

1- بخصوص صياغة المواد:

- إعادة صياغة المادة (44) من قانون الإجراءات الجزائية، وذلك بعدم اشتراط إذن قضائي في جرائم التلبس المتعلقة بالجرائم الإلكترونية، ضمانا للسرعة والفعالية، وذلك بإضافة فقرة ثالثة تُصاغ كما يأتي"...لا يتطلب وجود إذن صادر عن وكيل الجمهورية أو قاضي التحقيق في حالة التحرّي في الجنح المتلبس بها في جرائم المساس بأنظمة المعالجة الآلية للمعطيات، أو تلك التي ترتكب بأي وسيلة إلكترونية".

2- بخصوص التجريم والعقاب:

- تجريم إفساد سير نظام المعالجة الآلية للمعطيات بنص خاص والمتمثلة في أفعال: اعتراض (عرقلة – إعاقة– تعطيل) والتقاط المراسلات التي تتم داخل النظام المعلوماتي، وفعل تحريف (تغيير) سير الأنظمة المعلوماتية، إذ تعتبر هذه جرائم أساسية ترتكب ضد الأنظمة المعلوماتية.

- تجريم فعل التنصّت على النظام المعلوماتي، مثلما جرّمته المادة (3) من الاتفاقية الأوروبية للإجرام المعلوماتي.

- استحداث نص خاص ضمن القانون رقم:04-18 المؤرخ في:2004/12/25 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بهما، لتجريم أفعال الترويج والاتجار بالمخدرات الرقمية على غرار بعض التشريعات المقارنة، حيث تحول نظام التعاطي التقليدي للمخدرات والمؤثرات العقلية إلى نظام تعاطي إلكتروني أو رقمي، يحدث التأثير نفسه الذى تحدثه المخدرات الطبيعية أو الصناعية الأخرى، وربما أشدّ من ذلك. وهي أكثر خطورة من المخدرات التقليدية لما لها من تأثير مُدمّر على دماغ الانسان، قد يؤدي به إلى الوفاة مباشرة بعد استهلاكها.

– دعوة المشرع الجزائري إلى الإسراع في تحويل نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى نصوص قانونية، تداركا للفراغ التشريعي في هذا الشأن خاصة الجرائم التي لم ينص عليها المشرّع بعد، حيث تشمل الاتفاقية عديد الجرائم الإلكترونية نذكر منها:

- التزوير المعلوماتي.
- الإباحية الإلكترونية والجرائم المرتبطة.
- الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات.
- الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات .

3- بخصوص تسيير مقاهي الإنترنت: يشكل هذا الفضاء ملاذا آمنا للمجرم الإلكتروني لارتكاب جرائمه، حيث لا يترك أثرا للتعرّف عليه، وعليه نقترح:

– إلزام أصحاب مقاهي الإنترنت مسك دفتر مؤشر عليه من قبل الجهات المختصة، لتسجيل هوية الزبون ورقم جهاز الحاسوب وتاريخ ووقت ومدة استعماله، قصد الرجوع إليه لضرورة التحقيقات والتحريات ضمانا لعدم إفلات المجرم من العقاب.

– إلزام أصحاب مقاهي الإنترنت بتركيب كاميرات مراقبة لتسجيل حركة الزبائن، قصد التعرّف على المجرم الإلكتروني، ضمانا لعدم استعماله هوية مزورة، والاحتفاظ بهذه التسجيلات لمدة ستة(6) أشهر.

4- **بخصوص السلطات القضائية المكلفة بالبحث والتحرّي:** تتطور أساليب ارتكاب الجرائم الإلكترونية تبعا لتطور تكنولوجيات الإعلام والاتصال، مما يستدعي:

– الاهتمام بالتكوين النظري والتدريب العملي–إجراء دورات تدريبية– لأعضاء السلطة القضائية المكلفة بالبحث والتحرّي في الجرائم الإلكترونية، قصد اكتساب المهارات التقنية اللازمة والاستفادة من خبرات الدول الرائدة في مجال مكافحة هذا النوع المستحدث من الجرائم بكافة صُورها.

– توفير الوسائل الحديثة في مجال تكنولوجيات الإعلام والاتصال للسلطات القضائية المكلفة بالبحث والتحرّي، والعمل على تحديثها دوريا، تبعا للتطورات السريعة في هذا المجال، ضمانا لاستباق المجرم الإلكتروني.

– إنشاء مركز وطني متخصّص في التدريب على مكافحة كافة أشكال الجرائم الإلكترونية يُشرف عليه متخصّصون في مجال تكنولوجيات الإعلام والاتصال، من داخل الوطن وخارجه ويستفيد منه كل أعضاء الأجهزة القضائية.

وأخيرا وبرغم النقائص المسجلة، يمكن القول: بأنّ المشرّع الجزائري لازال في مرحلة بناء لمنظومة جزائية فعّالة ومتكاملة في مجال مكافحة الجرائم الإلكترونية، ويسير على ذلك بخطى ثابتة برغم التحديات الموضوعية والإجرائية التي يفرضها التعامل مع هذه البيئة الافتراضية.

قائمة المراجع:

أولا: المراجع باللغة العربية:

1- المؤلفات:

- أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي- دراسة مقارنة، دار النهضة العربية، القاهرة، مصر،2000.
- أحمد خليفة الملط، الجرائم المعلوماتية- دراسة مقارنة، دار الفكر الجامعي، الإسكندرية مصر ط2، 2006.
- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للطباعة والنشر والتوزيع الجزائر ط11، 2012.
- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة للطباعة والنشر والتوزيع الجزائر ط14، ج1، 2012.
- أحسن بوسقيعة، التحقيق القضائي، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط5 2004.
- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع الجزائر، ط1، 2006.
- أمير فرج يوسف المحامي، الجرائم المعلوماتية على شبكة الانترنيت، دار المطبوعات الجامعية الإسكندرية، مصر(ب.س.ط).
- أسامة أحمد المناعسة، جلال محمد الزغبي، صايل فاضل الهواوشة، جرائم الحاسب الآلي والإنترنيت- دراسة تحليلية مقارنة، دار وائل للنشر والتوزيع، الأردن، 2001.
- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني- دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، ط1، 2006.
- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الإسكندرية، مصر،2008.
- بشرى النية، الحماية القانونية لبرامج الحاسوب، جمعية نشر المعلومة القانونية والقضائية الرباط المملكة المغربية، 2009.

- جلال وفاء محمدين، دور البنوك في عمليات غسيل الأموال، دار الجامعة الجديدة للنشر الإسكندرية، مصر، 2004.
- جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية- دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2010.
- جميل عبد الباقي الصغير، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية القاهرة، مصر، ط1، 1992.
- جميل عبد الباقي الصغير، مدى كفاية نصوص قانون العقوبات والإجراءات الجنائي لمواجهة الإرهاب عبر الإنترنيت، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2008.
- هبة حسين محمد زايد، الحماية الجنائية للصفقات الإلكترونية، دار الكتب القانونية، القاهرة مصر، 2015.
- هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة مصر،1992.
- هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، النسر الذهبي القاهرة مصر، 2002.
- هلالي عبد الإله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلومات على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة، مصر، ط1، 2003.
- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية- دراسة مقارنة، مكتبة الآلات الحديثة، مصر، 1994.
- هشام فريد محمد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة مصر 1994.
- حنان ريحان المبارك المضحكي، الجرائم المعلوماتية- دراسة مقارنة، منشورات الحلبي الحقوقية بيروت، لبنان، ط1، 2014.
- حسين طاهري، الوجيز في شرح قانون الإجراءات الجزائية، دار المحمدية العامة، الجزائر ط2 1999.

- حسين محمدي بوادي، إرهاب الإنترنت الخطر القادم، دار الفكر الجامعي، الإسكندرية، مصر ط1، 2008.
- حسين فريجة، شرح قانون العقوبات الجزائري-جرائم الاعتداء على الأشخاص-جرائم الاعتداء على الأموال، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، ط2، 2009.
- حسين الغافري، ومحمد الألفي، جرائم الإنترنيت بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة، مصر، 2008.
- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنيت- دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2009.
- حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف للعلوم الأمنية، الرياض، السعودية ط1 . 2000
- حسن طاهر داود، الحاسب وأمن المعلومات، مركز البحوث، الرياض، السعودية، 2000 ص339.
- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة للنشر، الإسكندرية، مصر،2009.
- الطيب زروتي، القانون الدولي الخاص الجزائري مقارنا بالقوانين العربية، مطبعة الكاهنة الجزائر ج1، 2000.
- يوسف أبو الحجاج، أشهر جرائم الكمبيوتر والإنترنيت، دار الكتاب العربي، دمشق القاهرة مصر ط1، 2010.
- يوسف حسن يوسف، الجريمة الدولية للإنترنيت، المركز القومي للإصدارات القانونية، القاهرة مصر، ط1، 2011.
- يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي منشورات مركز كردستان للدراسات الاستراتيجية، السليمانية، مصر، 2007.
- يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والإنترنيت، دار العدالة، القاهرة مصر ط1، 2011.

- كوثر أحمد خالند، الإثبات الجنائي بالوسائل العلمية-دراسة تحليلية مقارنة، دار التفسير للنشر والإعلان، العراق،2007.
- محمد أمين فكيرين، أساسيات الحاسب الآلي، دار الراتب الجامعية، بيروت، لبنان،1993.
- محمد أمين الرومي، جرائم الكمبيوتر والإنترنيت، دار المطبوعات الجامعية، الإسكندرية مصر، 2003.
- محمد أمين الشوابكة، جرائم الحاسوب والإنترنيت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2007.
- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2007.
- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع عمان، الأردن، ط1، 2004.
- محمد حماد مرهج الهيتي، الجريمة المعلوماتية- دراسة مقارنة، دار الكتب القانونية، مصر- الإمارات، 2014.
- محمد حماد مرهج الهيتي، جرائم الحاسوب-دراسة تحليلية، دار المناهج للنشر والتوزيع عمان الأردن، ط1، 2006.
- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية القاهرة، مصر، ط1، 1994.
- محمد عبد الله أبو بكر سلامة، الكيان القانوني لغسل الأموال، المكتب العربي الحديث الإسكندرية، مصر، 2007.
- محمد عبدالله الرشدان، جرائم غسيل الأموال، دار قنديل للنشر والتوزيع ،الأردن، 2007.
- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، القاهرة، مصر، 2011.
- محمد عمر الشويرف، التجارة الإلكترونية في ظل النظام العالمي الجديد، دار زهرة للنشر والتوزيع، عمان، الأردن، ط1، 2013.

- محمد فتحي محمد أنور عزت، تفتيش شبكة الإنترنيت لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبارات التي تقع بواسطتها–دراسة مقارنة، المركز القومي للإصدارات القانونية القاهرة، مصر، ط1، 2012.
- محمد فتحي عيد، الإجرام المعاصر، أكاديمية نايف العربية للعلوم الأمنية، الرياض السعودية،1999.
- محمد صبحي نجم، شرح قانون العقوبات الجزائري–القسم الخاص، ديوان المطبوعات الجامعية بن عكنون، الجزائر، ط5، 2004.
- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2007.
- محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان الأردن 2005.
- محمود محمد لطفي صالح، المعلوماتية وانعكاساتها على الملكية الفكرية للمصنفات الرقمية–دراسة مقارنة، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر–الإمارات، 2014.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنيت، دار الكتب القانونية، مصر، 2006.
- منير محمد الجنبيهي وممدوح محمد الجنبيهي، جرائم الإنترنيت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر، 2004.
- مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، ماهيتها، مكافحتها–دراسة مقارنة، دار الكتب القانونية، مصر، 2005.
- مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنيت–دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، الكتاب الخامس، دار الكتب والوثائق القومية المصرية، ط1 2003.
- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، مصر ط1، 2009.

- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية بيروت لبنان، ط1، 2005.
- نادر عبد العزيز شافي، جريمة تبييض الأموال– دراسة مقارنة، المؤسسة الحديثة للكتاب طرابلس لبنان، 2005.
- نايز نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة الإسكندرية، مصر،2010.
- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنيت في مرحلة جمع الاستدلالات– دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر،2013.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1 ،2008.
- نعيم مغبغب، مخاطر المعلوماتية والإنترنيت–المخاطر على الحياة الخاصة وحمايتها–دراسة مقارنة، (ب.د.ن)، 1998.
- نعيم مغبغب، حماية برامج الكمبيوتر، منشورات الحلبي الحقوقية، لبنان، ط2، 2009.
- نصرالدين مروك، محاضرات في الإثبات الجنائي، درا هومة، الجزائر، ج2، 2004.
- نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، شركة المؤسسة الحديثة للكتاب، طرابلس، لبنان، ط1، 2011.
- سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الاثبات الجنائي– دراسة مقارنة، دار الكتب القانونية، مصر،2011.
- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية–دراسة تحليلية، دار الكتب القانونية دار شتات للنشر والبرمجيات، مصر، 2011.
- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنيت، دار الفكر الجامعي الإسكندرية مصر، 2007.
- سليم علي عبده، التفتيش في ضوء قانون أصول المحاكمات الجزائية الجديد–دراسة مقارنة منشورات زين الحقوقية، بيروت، لبنان، ط1، 2006.

- سعيد السيد قنديل، التوقيع الإلكتروني- ماهيته - صوره-حجيته في الإثبات، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ط2، 2006.
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، مصر، 2010.
- عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط1، 2011.
- عبد الله سليمان، دروس في شرح قانون العقوبات الجزائري-القسم الخاص، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، ط3، 1990.
- عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، ديوان المطبوعات الجامعية الجزائر، ط6، ج1، 2005.
- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنيت(الجرائم الإلكترونية)- دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنيت مع الإشارة الى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2007.
- عبد الهادي بن زيطة، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية، الجزائر ط1 2007.
- عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، دار المستقبل للنشر والتوزيع، الأردن ط1 2009.
- عبد المجيد جباري، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة والنشر والتوزيع، الجزائر،2012.
- عبد المنعم سليمان، النظرية العامة لقانون العقوبات، دار الجامعة الجديدة، الإسكندرية مصر،2000.
- عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الإلكترونية-دراسة قانونية قضائية مقارنة المركز القومي للإصدارات القانونية، القاهرة، مصر، ط1، 2012.

- عبد العزيز عياد، تبييض الأموال والقوانين والإجراءات المتعلقة بالوقاية منها ومكافحتها في الجزائر، دار الخلدونية ، الجزائر،2007.
- عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة-دراسة متعمقة ومقارنة في جرائم الهاتف المحمول-شبكة الإنترنيت والاتصالات-كسر شفرات القنوات الفضائية المدفوعة مقدما وذلك في قوانين فرنسا-مصر-الأردن-الإمارات-المغرب-عمان-قطر-البحرين-السعودية-فلسطين،المركز القومي للإصدارات القانونية، القاهرة، مصر، ط1 2011.
- عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنيت-دراسة مقارنة، منشأة المعارف، القاهرة، مصر، ط1، 2010.
- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنيت- دراسة معمقة في جرائم الحاسب الآلي والإنترنيت، دار بهجات للطباعة والتجليد، القاهرة، مصر 2009.
- عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة- دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، دار الفكر الجامعي، الإسكندرية، مصر 2008.
- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية- دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، دار النهضة العربية القاهرة مصر، ط1، 2009.
- عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار الفكر الجامعي الإسكندرية، مصر، ط1، 2003.
- عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي دار بهجات للطباعة والتجليد، مصر، ط1، 2009.
- عبد الفتاح بيومي حجازي، جريمة غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع دار الفكر الجامعي، الإسكندرية، مصر، 2005.
- عبد الصبور عبد القوي علي مصري، الجريمة الالكترونية، دار العلوم للنشر والتوزيع، القاهرة مصر، ط1، (ب.س.ط).

- عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، حق الملكية، دار إحياء التراث العربي، بيروت، ج8، 1952.
- عبد الرحمان أحمد محمد عثمان، مفاهيم نظم التشغيل، (ب، د، ن)، 2013.
- عبد الرحمن خلفي، محاضرات في قانون الاجراءات الجزائية، دار الهدى، عين مليلة الجزائر ط2، 2010.
- علي كحلون، الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الإلكترونية، دار إسهامات في أدبيات المؤسسة، تونس،2002.
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة الإسكندرية، مصر،2010.
- علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة منشورات زين الحقوقية، بيروت، لبنان، ط1، 2013.
- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية المكتب الجامعي الحديث، الإسكندرية، مصر، 2012.
- علي لعشب، الإطار القانوني لمكافحة غسل الأموال، ديوان المطبوعات الجامعية، الجزائر 2007.
- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا- دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2010.
- عمر محمد بن يونس، التحكم في جرائم الحاسوب وردعها(المراقبة الدولية للسياسة الجنائية – ملخص الترجمة العربية لمرشد الأمم المتحدة لعام1999)، دار النهضة العربية، القاهرة مصر، ط1، 2005.
- عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية دار النهضة العربية، القاهرة، مصر، ط2، 1995.
- عماد مجدي عبد الملك، جرائم الكمبيوتر والإنترنيت، دار المطبوعات الجامعية، الإسكندرية مصر، 2011.

- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشأة المعارف، الإسكندرية، مصر، (ب.س.ط).
- عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، مصر، 2015.
- فاضل زيدان، سلطة القاضي الجنائي في تقدير الأدلة، دار الثقافة للنشر والتوزيع، عمان الأردن،1999.
- فؤاد أمين السيد محمد، جرائم الاتصالات وكهرومغناطيسية الموجات- دراسة تحليلية وتشريعية مقارنة، دار النهضة العربية، القاهرة، مصر، 2014.
- فؤاد حسن العزيزي، الجرائم المعلوماتية-دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر 2015.
- فريد هـ.كيت، الخصوصية في عصر المعلومات- ترجمة محمد محمود شهاب، مركز الأهرام للترجمة والنشر، القاهرة، مصر، ط1، 1999.
- فريد منعم جبور، حماية المستهلك عبر الإنترنيت ومكافحة الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2010.
- رياض فتح الله بصله، جرائم بطاقة الائتمان، دار الشروق، القاهرة، مصر، ط1، 1995.
- رمزي نجيب القسوس، غسيل الأموال جريمة العصر-دراسة مقارنة ، دار وائل للطباعة والنشر عمان، الأردن، 2002.
- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2012.
- الشحات ابراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية بحث فقهي مقارن، دار الفكر الجامعي، الإسكندرية، مصر، ط1، 2011.
- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجريمة الإلكترونية، دار الفكر الجامعي الإسكندرية، مصر،2009.
- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، مصر، 2008.

- خالد ممدوح أبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، ط1 2009.
- خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء قانون حماية الملكية الفكرية–دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2005.

2- الرسائل:

أ- أطروحة الدكتوراه:

- محمد خليفة، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، أطروحة دكتوراه، كلية الحقوق، قسم القانون الخاص، جامعة باجي مختار، عنابة، الجزائر،2011.
- سامح أحمد بلتاجي موسى، الجوانب الاجرائية للحماية الجنائية لشبكة الانترنيت، رسالة دكتوراه كلية الحقوق، جامعة الاسكندرية، مصر،2010.
- عبد العزيز نويري، الحماية الجزائية للحياة الخاصة، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر،2011.
- عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنيت، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، القاهرة، مصر، 2004.
- فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه كلية الحقوق، جامعة الجزائر1، 2011.
- فضيلة عاقلي، الحماية القانونية للحق في حرمة الحياة الخاصة، دراسة مقارنة، أطروحة دكتوراه كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2012.
- القحطاني خالد بن مبارك القروي، التعاون الأمني الدولي ودوره في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه، قسم فلسفة العلوم الأمنية، جامعة نايف للعلوم الأمنية، الرياض السعودية 2006.

ب- المذكرات:

ب1- مذكرات الماجستير:

- يوسف صغير، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية جامعة مولود معمري، تيزي وزو، الجزائر، 2013.
- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر باتنة، 2013 الجزائر، ص124.

- سمية ديمش، التجارة الإلكترونية حقيقتها وواقعها في الجزائر، مذكرة ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، قسم العلوم الاقتصادية، جامعة منتوري، قسنطينة، الجزائر 2011.

ب2- مذكرات الماستر:

- سارة قادري، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماستر أكاديمي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر ،2014.

3- المقالات العلمية:

- أمجد حسان، الفيروسات ارهابا تهدد أنظمة المعلومات، مجلة، دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد4، السداسي الأول،2011.
- بشرى النية ،الحماية القانونية لبرامج الحاسوب، منشورات جمعية نشر المعلومة القانونية والقضائية–سلسلة الدراسات والأبحاث، المغرب، العدد10، مارس2009.
- جميلة محلق، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، جامعة باجي مختار، عنابة الجزائر، العدد42، جوان2015.
- حسين براهيم، الحاسب الآلي وتحديات القرن الحادي والعشرون، مجلة مركز بحوث الشرطة أكاديمية الشرطة، مصر، العدد الرابع عشر، 1998.
- حسن مظفر الرزو، الأمن المعلوماتي(معالجة قانونية أولية)، مجلة الأمن والقانون، أكاديمية شرطة دبي، الامارات العربية المتحدة، العدد 1، السنة الثانية عشر، جانفي 2004.
- مها كامل، عمليات غسيل الأموال، الإطار النظري، مجلة السياسة الدولية، القاهرة، مصر، العدد 146، سنة2001.
- محمد مزاولي، المسؤولية الجنائية للأشخاص المعنوية عن الجرائم الإلكترونية في القانون الجزائري، مجلة، دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة الجزائر، العدد 01، 2009.
- محمد علي سالم و حسون عبيد هجيج، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية كلية القانون، جامعة بابل، العراق، المجلد14، العدد6، 2007.

- محمد خليفة، خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 01، 2009.
- منصور بن عبد الرحمن بن عسكر، دور المؤسسات الاجتماعية في التبصير من جرائم تقنية المعلومات، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة الجزائر، العدد6، الثلاثي الأول، 2012.
- نادية سحتوت، التنظيم القانوني للجريمة المعلوماتية–أدلة اثبات الجريمة المعلوماتية، مجلة دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 01، 2009.
- عبد الحليم بوشكيوة، آليات مكافحة الجرائم الماسة بالأخلاق والآداب العامة على الانترنت مجلة، دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر العدد 1، 2009.
- عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، مجلة، دراسات و أبحاث كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 01، 2009.
- فاطمة زهرة بوعناد، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة، الندوة للدراسات القانونية، قسنطينة، الجزائر، العدد1، 2013.
- فايز الظفيري، الأحكام العامة للجريمة الإلكترونية، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مصر، السنة الرابعة والأربعون، العدد2، 2002.
- فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الانسانية، جامعة قسنطينة1، الجزائر،العدد33، جوان 2010.
- رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجلة، دراسات وأبحاث، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر، العدد 01، 2009.
- ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة و التطبيقات مجلة سلسلة الدراسات القانونية في المجال المعلوماتي، مطبعة دور الوراقة الوطنية، المملكة المغربية، العدد01، سنة2011.
- غنام محمد غنام، الحماية الإدارية والجنائية للأفراد عند تجميع بياناتهم الشخصية في أجهزة الكمبيوتر، مجلة الأمن والقانون، أكاديمية شرطة دبي، الإمارات العربية المتحدة، السنة الحادية عشر، العدد2، 2003.

4- الملتقيات:

– جلول بن عناية وحواسني يمينة، مفاهيم أساسية حول الإنترنيت والتجارة الإلكترونية، الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر – عرض تجارب دولية –المركز الجامعي خميس مليانة، الجزائر يومي:26–27 أفريل 2011 .

– جميل أحمد ورشام كهينة، بطاقة الائتمان كوسيلة من وسائل الدفع في الجزائر، الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر – عرض تجارب دولية –المركز الجامعي خميس مليانة، الجزائر، يومي:26–27 أفريل 2011.

– يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، ورقة عمل مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، هيئة تنظيم الاتصالات، مسقط، سلطة عمان، يومي 2 و 4 أفريل، سنة 2006.

– محرز نورالدين ومريم صيد، نظام الدفع الإلكتروني ودوره في تفعيل التجارة الإلكترونية، الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية واشكالية اعتماد التجارة الإلكترونية في الجزائر – عرض تجارب دولية –المركز الجامعي خميس مليانة، الجزائر يومي:26–27 أفريل 2011.

– عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، من 12 الى 14 نوفمبر 2007، الرياض، السعودية.

– عبد الرحيم وهيبة، تقييم وسائل الدفع الالكترونية ومستقبل وسائل الدفع التقليدية في ظل وجودها، الملتقى العلمي الدولي الرابع حول عصرنة نظام الدفع في البنوك الجزائرية واشكالية اعتماد التجارة الإلكترونية في الجزائر – عرض تجارب دولية –المركز الجامعي خميس مليانة الجزائر، يومي:26–27 أفريل 2011.

5- النصوص الرسمية:

أ- الدساتير:

- دستور الجزائر لسنة 1963 الصادر في:1963/09/08.
- القانون رقم:16–01 المؤرخ في:2016/03/06 يتضمن التعديل الدستوري.

ب- الاتفاقيات:

- الاعلان العالمي لحقوق الانسان الصادر في:1948/12/10، انضمت إليه الجزائر غداة الاستقلال بموجب نص المادة (11) من دستور 1963 الصادر بتاريخ:1963/09/08.
- اتفاقية تريبس: بتاريخ: 1994/04/15.
- اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم:95-41 المؤرخ في 28 يناير 1995 (ج. ر) رقم: 7 المؤرخة في: 1995/02/15.
- اتفاقية برن لحقوق المؤلف لسنة 1882 المعدلة والمتممة، صادقت عليها الجزائر مع التحفظ بموجب المرسوم الرئاسي رقم:341/97 المؤرخ في:1997/09/13، (ج. ر) رقم:61 المؤرخة في:1997/09/14.
- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم:2000/11/15، صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم:04-165 المؤرخ في:2004/06/08.
- اتفاقية ثنائية بين الجزائر وفرنسا حول التعاون في مجال مكافحة الجرائم المنظمة، المرسوم الرئاسي رقم:07-375 المؤرخ في:2007/12/01، الجريدة الرسمية العدد:77 المؤرخة في:2007/12/09.
- الاتفاقية الدولية لقمع أعمال الإرهاب النووي، صادقت عليها الجزائر مع التحفظ بموجب المرسوم الرئاسي رقم:10-270 المؤرخ في:2010/11/10، (ج.ر) رقم:68 المؤرخة في:2010/11/10.
- الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الوطنية، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم:14-251 المؤرخ في:2014/09/08، (ج.ر) رقم:56 المؤرخة في:2014/09/25.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ:2010/12/21، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم:14-252 المؤرخ في:2014/09/08، (ج.ر) رقم:57 المؤرخة في:2014/09/28.

ج- القوانين والأوامر:

ج.1-القوانين:

- قانون العقوبات المصري الصادر في: 31 يوليو 1937 المعدل والمتمم.
- القانون رقم:2000-03 المؤرخ في:2000/08/05، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، (ج.ر) رقم:48 المؤرخة في:2000/08/06.

- القانون رقم:2000-83 المؤرخ في 09 أوت 2000المتعلق بالمبادلات والتجارة الإلكترونية، الرائد الرسمي للجمهورية التونسية، العدد:64 المؤرخ في:2000/08/11.
- القانون رقم: 01-09 المؤرخ في: 2001/06/26 يعدل ويتمم الأمر رقم: 66-156 المؤرخ في: 1966/06/08، والمتضمن قانون العقوبات، (ج.ر) رقم:34 المؤرخة في:2001/06/27.
- القانون العربي النموذجي الموحد في بشأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصال لسنة 2003.
- بالقانون رقم:04-14 المؤرخ في:2004/11/10، المعدل والمتمم لقانون الإجراءات الجزائية (ج.ر) رقم: 71 المؤرخة في: 2004/11/10
- القانون رقم: 04-15 المؤرخ في: 2004/11/10 يعدل ويتمم الأمر رقم: 66-156 المؤرخ في: 8 يونيو 1966 والمتضمن قانون العقوبات، (ج.ر) رقم:71 المؤرخة في:2004/11/10.
- القانون رقم:04-18 المؤرخ في:2004/12/25 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بهما ، (ج.ر) رقم:83 المؤرخة في:2004/12/26.
- القانون رقم: 05-01 المؤرخ في: 2005/02/06 يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، (ج.ر) رقم: 11، المؤرخة في: 09 فبراير 2005.
- القانون رقم:05- 10 المؤرخ في:2005/06/20 يعدل ويتمم الأمر رقم:75-58 المؤرخ في:1975/09/26 والمتضمن القانون المدني المعدل والمتمم،(ج.ر) رقم:44 المؤرخة في:2005/06/26.
- القانون رقم:05-11 المؤرخ في:2005/07/17 المتعلق بالتنظيم القضائي، (ج.ر) رقم:51 المؤرخة في:2005/07/20.
- نظام بنك الجزائر رقم:05-07 المؤرخ في:2005/12/28.
- القانون رقم:06-01 المؤرخ في: 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته، (ج.ر) رقم:14 المؤرخة في:2006/03/08.
- القانون رقم:06-22 المؤرخ في:2006/12/20، يعدل ويتمم الأمر رقم: 66-155 المؤرخ في: 1966/06/08، والمتضمن قانون الإجراءات الجزائية، (ج.ر) رقم:84 المؤرخة في:2006/12/24.
- القانون رقم:06-23 المؤرخ في:2006/12/20 يعدل ويتمم الأمر رقم: 66-156 المؤرخ في: 1966/06/08، والمتضمن قانون العقوبات، (ج.ر) رقم:84 المؤرخة في:2006/12/24.
- نظام مكافحة الجرائم المعلوماتية السعودي الصادر في:2007/03/26.

- القانون رقم: 08-01 المؤرخ في:2008/01/23، يتمم القانون رقم:83-11 المؤرخ في:1982/07/02 والمتعلق بالتأمينات الاجتماعية، (ج.ر) رقم:04، المؤرخة في: 2008/01/27.
- القانون رقم:09-01 المؤرخ في:2009/02/25، يعدل ويتمم الأمر رقم: 66-156 المؤرخ في: 1966/06/08، والمتضمن قانون العقوبات، (ج.ر) رقم:15 المؤرخة في:2009/03/08.
- القانون رقم: 09 – 04 المؤرّخ في:2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (ج.ر) رقم:47، المؤرخة في:2009/08/16.
- القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية الذي اعتمد بقرار مجلس وزراء العدل العرب رقم: 812/د25 بتاريخ 2009/11/19.
- القانون رقم:15-04 المؤرخ في:2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، (ج.ر) رقم:06 المؤرخة في:2015/02/10.

ج.2 الأوامر:

- الأمر رقم:66-155 المؤرخ في:08 يونيو 1966 الذي يتضمن قانون الإجراءات الجزائية المعدل والمتمم.
- الأمر رقم:66-156 المؤرخ في:08 يونيو 1966 المتضمن قانون العقوبات، المعدل والمتمم.
- الأمر رقم:75-58 المؤرخ في:26 سبتمبر 1975 يتضمن القانون المدني المعدل والمتمم.
- الأمر رقم:75-59 المؤرخ في:26 سبتمبر 1975 والمتضمن القانون التجاري، المعدل والمتمم.
- الأمر رقم:03-05 المؤرخ في: 2003/06/19 يتعلق بحقوق المؤلف والحقوق المجاورة، (ج.ر) رقم: 44، المؤرخة في:2003/06/23.
- الأمر رقم:03-11 المؤرخ في 2003/06/26 المعدل والمتمم لقانون القرض.
- الأمر رقم:03-06 المؤرخ في:2003/07/19 يتعلق بالعلامات، (ج.ر) رقم:44، المؤرخة في:2003/07/23.
- الأمر رقم:03-07 المؤرخ في:2003/07/19 يتعلق ببراءات الاختراع، (ج.ر) رقم:44 المؤرخة في:2003/07/23.
- الأمر رقم:05-06 المؤرخ في: 2005/08/23 يتعلق بمكافحة التهريب،(ج.ر) رقم:59 المؤرخة في:2005/08/28.

د-النصوص التنظيمية:

د.1: المراسيم الرئاسية:

- المرسوم الرئاسي رقم :67/89 المؤرخ في:1989/05/16، المتضمن انضمام الجزائر إلى العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، والعهد الدولي الخاص بالحقوق المدنية والسياسية والبروتوكول الاختياري المتعلق بالعهد الدولي الخاص بالحقوق المدنية والسياسية الموافق عليها من طرف الجمعية العامة للأمم المتحدة بتاريخ:1966/12/16، (ج.ر) رقم:20 المؤرخة في:1989/05/17.
- المرسوم الرئاسي رقم: 183-04 المؤرخ في: 2004/06/26 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، (ج.ر) رقم:41 المؤرخة في:2004/06/27.
- المرسوم الرئاسي رقم:04-432 المؤرخ في:12/29/ 2004 يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي.
- المرسوم الرئاسي رقم:15-261 المؤرخ في:10/08/ 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (ج.ر) رقم:53 المؤرخة في:2015/10/08 .

د.2-المراسيم التنفيذية:

- المرسوم التنفيذي رقم:98-257 المؤرخ في:1989/08/25 يضبط شروط وكيفيات إقامة خدمات إنترنات واستغلالها، (ج.ر) رقم:63 المؤرخة في:1989/09/26.
- المرسوم التنفيذي رقم06-348 المؤرخ في:2006/10/05 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق، (ج.ر) رقم: 63 المؤرخة في:2006/10/08.
- المرسوم التنفيذي رقم:07-162 المؤرخ في:2007/05/30 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، (ج.ر) رقم:37 المؤرخة في:2007/07/07.

هـ- القرارات الوزارية المشتركة:

- القرار الوزاري المشترك المؤرخ في:2007/04/14، يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، (ج.ر) رقم:36 المؤرخة في:03 يونيو 2007.

6- الوثائق:

- التوجيه الأوربي رقم: 93-1999 بشأن الإطار المشترك للتواقيع الإلكترونية الصادر بتاريخ: 1999/12/13.
- المذكرة التفسيرية للاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي لسنة2001.

7- مواقع الإنترنت:

يونس عرب، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها، بحث متوفر على الموقع الآتي:

- http://www.abhatoo.net.ma

يونس عرب، البنوك الخلوية، التجارة الخلوية، المعطيات الخلوية، ثورة جديدة تنبئ بانطلاق عصر ما بعد المعلومات، بحث متوفر على الموقع الآتي:

- http://www.abhatoo.net.ma

يونس عرب، جرائم الكمبيوتر والإنترنت المعنى والخصائص والصور واستراتيجية المواجهة القانونية، بحث متوفر على الموقع الآتي:

- http://www.abhatoo.net.ma

المخدرات الرقمية..خطر إدمان جديد، متوفر على الرابط الآتي:

-*http://www.alarabiya.net/ar/last-page/2014/10/30/%D8%A7%D9%84%D9%85%D8%AE%D8%AF%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A%D8%A9-%D8%AE%D8%B7%D8%B1-%D8%A5%D8%AF%D9%85%D8%A7%D9%86-%D8%AC%D8%AF%D9%8A%D8%AF-.html*

حصيلة قدمتها شركة اتصالات الجزائر للفترة الممتدة من 2003 إلى 2013، متوفرة على الرابط الآتي:

-*http://www.algerietelecom.dz/AR/?p=at_histoire_realisations*

أمريكي يبلغ عن جريمة قتل شاهدها مباشرة على الانترنت، متوفر على الرابط الآتي:

-*http://www.al-jordan.com/?p=1104*

العاقد غريب أحمد، جرائم الإهانة والقذف والسب، دراسة قانونية منشورة على الموقع الرسمي للنيابة الإدارية المصرية على الرابط الآتي:

http://ap.gov.eg/elmaktaba/Crimes%20of%20insult%20and%20defamation%20and%20insult.pdf

الانطلاق الرسمي لخدمة الدفع الإلكتروني في الجزائر، متوفر على الرابط الآتي:

- http://www.aps.dz/ar/economie/34600-%D8%A7%D9%84%D8%A5%D8%B7%D9%84%D8%A7%D9%82-%D8%A7%D9%84%D8%B1%D8%B3%D9%85%D9%8A-%D9%84%D8%AE%D8%AF%D9%85%D8%A9-%D8%A7%D9%84%D8%AF%D9%81%D8%B9-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A

توقيع اتفاقية ثنائية بين الجزائر وفرنسا بشأن التعاون القضائي في مجال مكافحة الإجرام المنظم:

- http://www.aps.dz/ar/economie/34634-%D8%A7%D9%84%D8%AC%D8%B2%D8%A7%D8%A6%D8%B1-%D9%81%D8%B1%D9%86%D8%B3%D8%A7-%D8%A7%D9%84%D8%AA%D9%88%D9%82%D9%8A%D8%B9-%D8%A8%D8%A8%D8%A7%D8%B1%D9%8A%D8%B3-%D8%B9%D9%84%D9%89-%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D8%A9-%D8%AA%D8%B9%D8%A7%D9%88%D9%86-%D9%82%D8%B6%D8%A7%D8%A6%D9%8A-%D9%81%D9%8A-%D8%A7%D9%84%D9%85%D8%AC%D8%A7%D9%84-%D8%A7%D9%84%D8%AC%D9%86%D8%A7%D8%A6%D9%8A

تفكيك أخطر شبكة إلكترونية لتجنيد الجزائريين في "داعش"، خبر منشور على الموقع الرسمي لوكالة الأنباء الجزائرية:

- *http://www.aps.dz/ar*

المخابرات الألمانية تجسست على دبلوماسي ألماني وحلفاء بارزين، خبر منشور على الرابط الآتي:

- *http://ara.reuters.com/article/worldNews/idARAKCN0T014E20151111*

تقرير نشاطات سلطة الضبط للبريد والمواصلات السّلكية واللاّسلكية لسنة 2014، منشور على الرابط الآتي:

- *http://www.arpt.dz/ar/pub/raa*

تقرير سلطة الضبط للبريد والمواصلات السلكية واللاسلكيةلسنة2015 على الرابط الآتي:

- *http://www.arpt.dz/fr/#*

مهام سلطة الضبط للبريد والمواصلات السّلكية واللاّسلكية، منشورة على الرابط الآتي:

- *http://www.arpt.dz/ar/arpt/bref*

القائمة الرسمية لمزودي خدمة النفاذ لشبكة الإنترنت، منشورة على الموقع الرسمي لسلطة الضبط للبريد والمواصلات السّلكية واللاّسلكية على الرابط الآتي:

- *http://www.arpt.dz/ar/obs/prest/?c=fai*

مفهوم الحاسوب فائق السرعة، منشور على الرابط الآتي:

- *https://ar.wikipedia.org/wiki/%D8%AD%D8%A7%D8%B3%D9%88%D8%A8_%D9%81%D8%A7%D8%A6%D9%82*

مفهوم الهاتف النقال(الخلوي)، منشور على الرابط الآتي:

- *https://ar.wikipedia.org/wiki/%D9%87%D8%A7%D8%AA%D9%81_%D9%85%D8%AD%D9%85%D9%88%D9%84*

تعريف لشبكة الحاسوب، منشور على الرابط الآتي:

- *https://ar.wikipedia.org/wiki/%D8%B4%D8%A8%D9%83%D8%A9_%D8%AD%D8%A7%D8%B3%D9%88%D8%A8*

مفهوم شبكة الواي– فاي*(wifi)*، منشور على الرابط الآتي:

- *https://ar.wikipedia.org/wiki/%D9%88%D8%A7%D9%8A-%D9%81%D8%A7%D9%8A*

تعريف تقنية البلوتوث *(bluetooth)*، *منشور على الرابط الآتي:*

- *https://ar.wikipedia.org/wiki/%D8%A8%D9%84%D9%88%D8%AA%D9%88%D8%Ab*

مفهوم المخدرات الرقمية، منشور على الرابط الآتي:

- *https://ar.wikipedia.org/wiki/%D9%85%D8%AE%D8%AF%D8%B1_%D8%B1%D9%82%D9%85%D9%8A*

تعريف الشبكة الداخلية إنترنت(intranet)، منشور على الرابط الآتي:

- *https://ar.wikipedia.org/wiki/%D8%A5%D9%86%D8%AA%D8%B1%D8%A7%D9%86%D8%AA*

مفهوم تقنية تسجيل الصوت وإعادة إنتاجه، منشور على الرابط الآتي:

- *https://ar.wikipedia.org/wiki/%D8%AA%D8%B3%D8%AC%D9%8A%D9%84_%D8%A7%D9%84%D8%B5%D9%88%D8%AA_%D9%88%D8%A5%D8%B9%D8%A7%D8%AF%D8%A9_%D8%A5%D9%86%D8%AA%D8%A7%D8%AC%D9%87*

خريطة ثلاثية الأبعاد أعدتها شركة *(Kaspersky)* عن التهديدات الإلكترونية المختلفة التي تصيب الدول ومنها الجزائر، وهذا خلال الثلاثي الأول من سنة 2014 ، منشورة على الرابط الآتي:

- *https://cybermap.kaspersky.com/*

إحصاءات الجرائم الإلكترونية في الجزائر لسنة2014، منشورة على الرابط الآتي:

- http://www.dgsn.dz/?%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A-%D9%8A%D8%B9%D8%A7%D9%84%D8%AC,4800

افتتاح أشغال الدورة الـ22 للندوة الإقليمية الإفريقية للإنتربول بوهران، بتاريخ:2013/09/10 منشور على الرابط الآتي:

- http://www.dgsn.dz/?%D8%A7%D9%81%D8%AA%D8%AA%D8%A7%D8%AD-%D8%A3%D8%B4%D8%BA%D8%A7%D9%84,2439

عثمان لحياني، ورشة عمل حول: "الجريمة الإلكترونية وأمن المعلومات"، حيث قدمت الاستخبارات الأمريكية دورة تدريبية لقضاة وضباط الشرطة القضائية على محاربة هذه الجرائم منشورة على الرابط الآتي:

- http://www.djazairess.com/elkhabar/235287

قضية المدون الجزائري (ع.غ.ع) الذي تُوبع في سنة 2015 من أجل جريمة "إهانة وقذف هيئات نظامية عن طريق الكتابة في مواقع التواصل الاجتماعي، منشور على الرابط الآتي:

- www.djazairess.com/essalam/42690

حافظ بن زلاط، التنصت الهاتفي في ظل قانون الإجراءات الجزائية، بحث منشور على الرابط الآتي:

- http://www.droitetentreprise.org/web/%D8%A7%D9%84%D8%AA%D9%86%D8%B5%D8%AA-%D8%A7%D9%84%D9%87%D8%A7%D8%AA%D9%81%D9%8A-%D9%81%D9%8A-%D8%B8%D9%84-%D9%82%D8%A7%D9%86%D9%88%D9%86-

%D8%A7%D9%84%D8%A5%D8%AC%D8%B1%D8%A7%D8%A1%D8%A7%D8%AA-%D8%A7/

التقرير الاستراتيجي الدولي لمراقبة المخدرات مارس 2012، مكتب شؤون المخدرات الدولية وتنفيذ القوانين–الولايات المتحدة الأمريكية، منشور على الرابط الآتي:

- *http://www.ginad.org/ar/info/researches/2826/International-Narcotics-Control-Strategy-Report-March-2012*

داريل بانثيير، استمرار القرصنة: تبعاتها على الإبداع وعلى الثقافة وعلى التنمية المستدامة، بحث منشور على الرابط الآتي:

- *https://www.google.com/url?q=http://portal.unesco.org/culture/es/files/29853/11467333771bull_3_2005_ar.pdf/bull_3_2005_ar.pdf&sa=U&ved=0ahUKEwjk-JXM37TPAhWE1RoKHaldCUYQFggEMAA&client=internal-uds-cse&usg=AFQjCNHwg1ANz88pxlufSbBFaymwJLj8FQ*

مركز الشكاوى الخاصة بجرائم الإنترنت *(IC3)* ، على الموقع الرسمي الآتي:

- *https://www.ic3.gov/default.aspx*

تعريف الاتحاد الدولي للاتصالات: "للاتصالات اللاّسلكية"، منشور على الرابط الآتي:

- *www.itu.int/ar/pages/default.aspx*

تقرير الاتحاد الدولي للاتصالات لسنة2013، منشور على الرابط الآتي:

- *http://telecomworld.itu.int/outcomes/2013-report/*

ظاهرة استغلال الأطفال جنسياً عبر الإنترنت (*Child Pornography on the Internet*) منشورة على الرابط الآتي:

- *https://www.justice.gov/criminal-ceos/child-pornography*

دراسة عليمة تثبت خطر المشاهد الجنسية على دماغ الإنسان، منشورة على الرابط الآتي:

- *http://www.kaheel7.com/ar/index.php/2010-02-02-22-17-58/1577-2013-12-31-03-28-32*

الاتفاقية العربية لمكافحة الإرهاب، منشورة على موقع جامعة الدول العربية على الرابط الآتي:

- *http://www.lasportal.org/ar/legalnetwork/Pages/agreements_details.aspx?RID=68*

الندوة الدولية حول: "الأمن السيبراني بالجزائر"، من تنظيم قيادة الدرك الوطني، وذلك يومي 24 و25 ماي 2016 بالنادي الوطني للجيش ببني مسوس بالجزائر العاصمة، منشورة على الموقع الرسمي لقيادة الدرك الوطني على الرابط الآتي:

- *http://www.mdn.dz/site_principal/index.php?L=ar#undefined*

تقرير مركز شكاوي جرائم الإنترنت *(the internet crime complaint center)* لسنة2013، منشور على الرابط الآتي:

- *https://pdf.ic3.gov/2013_IC3Report.pdf*

خدمة " الشكوى المسبقة والاستعلام عن بعد " أطلقتها قيادة الدرك الوطني سنة 2016 متوفرة على الرابط الآتي:

- *https://ppgn.mdn.dz/prep.php*

إجراء أول محاكمة قضائية عن بعد بمحكمة القليعة بالجزائر في شهر أكتوبر2015، منشور على الرابط الآتي:

- *http://www.radioalgerie.dz/news/ar/article/20151008/54527.html*

نصوص الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي ببودابيست 2001، منشورة على الموقع الرسمي للمجلس الأوروبي على الرابط الآتي:

- https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008156d

مشعل بن عبدا الله القدهي، المواقع الإباحية على شبكة الإنترنت وأثرها على الفرد والمجتمع بحث منشور على الرابط الآتي:

- https://saaid.net/mktarat/abahiah/1.htm

حسين بن سعيد الغافري، الإنترنت وآفة المخدرات، بحث منشور على الرابط الآتي:

- http://www.shaimaaatalla.com/vb/showthread.php?t=3939

عبدالله بن عبدالعزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، منشور على الرابط الآتي:

- http://www.shaimaaatalla.com/vb/showthread.php?t=3937

ماهية المخدرات الرقمية، بحث منشور على الرابط الآتي:

- http://www.tech-wd.com/wd/2014/11/15/%D8%A7%D9%84%D9%85%D8%AE%D8%AF%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A%D8%A9-digital-drugs-0/

مؤتمر كراكاس بفنزويلا سنة1980 تحت شعار:" الوقاية من الجريمة ونوعية الحياة" بشأن مكافحة الأشكال الجديدة للإجرام، منشور على الموقع الرسمي للأمم المتحدة على الرابط الآتي:

-http://www.un.org/ar/events/crimecongress2015/about.shtml

المعاهدة النموذجية لتبادل المساعدة في المسائل الجنائية والبروتوكول الاختياري بشأن عوائد الجريمة، منشورة على الموقع الرسمي للأمم المتحدة على الرابط الآتي:

- *http://www.un.org/arabic/documents/basic/treaties.html*

- مراسلة السيد الوزير الأول رقم:2981 المؤرخة في:2016/09/22، المتعلقة بقرصنة معلومات تستهدف مؤسسات الدولة، منشورة على الموقع الرسمي لجامعة باجي مختار عنابة على الرابط الآتي:

- *http://www.univ-annaba.dz/component/k2/item/485-bulletin-d-information-relatif-%C3%A0-une-forme-de-piratage-informatique-ciblant-les-institutions-de-l-%C3%A9tat.html*

تقرير مكتب الأمم المتحدة الخاص بالمخدرات والجريمة *(UNODC)* لسنة 2014، منشور على الرابط الآتي:

- *http://www.unodc.org/wdr2014/*

قرار الجمعية العامة للأمم المتحدة رقم:(63/55) بتاريخ:2001/01/22 والمتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، متوفر على الموقع الرسمي للأمم المتحدة على الرابط الآتي:

- *http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/55/63*

دراسة أُجريت سنة 2009 حول توجهات مستعملي شبكة الإنترنت في الجزائر، منشورة على الرابط الآتي:

- *www.webdialna.com/pdf/presse.pdf*

مهام وأهداف المنظمة العالمية للملكية الفكرية، منشورة على الموقع الرسمي للمنظمة على الرابط الآتي:

- *http://www.wipo.int/about-wipo/ar/what_is_wipo.html.*

8- الأحكام والقرارات القضائية:

- الحكم رقم: 10/05272الصادر عن محكمة باتنة بتاريخ:2010/06/01.
- الحكم رقم: 10/07357 الصادر عن محكمة عنابة بتاريخ: 2010/06/28.

Deuxièmement: Références en Français: ثانيا: المراجع باللغة الأجنبية:

1- Ouvrages :

- ADEL BRAHMI , Signature électronique et Droit, édition MS, Tunisie, 2004.
- Alain Bensoussan, L'informatique et le droit, Memento Guide, édition HERMES, Paris, France, Tome 1, 1994.
- Alain Bensoussan, Internet aspects juridique, édition HERMES,Paris,France, 2ème édition ,1998
- Ali EL AZZOUZI, La Cybercriminalité au Maroc, Bishoop solution, Casablanca, Maroc, 1ere édition,2010.
- André Lucas et Jean Devèze et Jean Frayssinet , Droit de L'informatique et de L'internet, Presse Universitaire de France, 2001.
- CHRISTIANE FERAL-SCHUHL,Le droit a L'épreuve De L'INTERNET, DALLOZ, DUNOD, Paris,France, 2eme édition ,2000
- CHRISTIANE FERAL-SCHUHL,Le droit a L'épreuve De L'INTERNET, DALLOZ, France, Quatrième édition, 2006.
- Christophe Emmanuel Lucy, L'odeur de l'argent sale : dans les coulisses de la criminalité financière, , Eyrolles société, Paris, 2003.
- David FOREST et Gautier Kaufman, Droit de L'informatique,Gualino éditeur, Extenso édition, France,2010.
- Jean Larguier et Philippe Conte et Anne-Marie Larguier, Droit pénal spécial, Mémento Dalloz, ,France, 13 édition ,2005.
- Myriam Quéméner et Joel Ferry, Cybercriminalité Défi mondial, , Economica, France, 2e édition, 2009.
- Myriam Quéméner et Yves Charpenel, Cybercriminalité Droit pénal appliqué, Economica, France,2010.

- *Nidal El Chaer, La Criminalité Informatique Devant La Justice Pénale, édition juridique sader, Beyrouth, Liban,2004.*
- *Olivier Jerez, Le blanchiment de l'argent, BANQUE édition, France, 2ème édition, 2003.*

2- Articles:

- *Christiane Féral Schuhl, La collecte de la preuve numérique en matière pénale, Actualité Juridique Pénal, Editions Dalloz, 2009.*
- *David Bénichou, Cybercriminalité : jouer d'un nouvel espace sans frontière, Actualité Juridique Pénal, Editions Dalloz, 2009.*
- *Frédérique Chopin, Les politiques publiques de lutte contre la cybercriminalité, Actualité Juridique Pénal, Editions Dalloz, 2009.*
- *Myriam Quemener, Réponses pénales face à la cyber pédopornographie, Actualité Juridique Pénal, Editions Dalloz, 2009.*
- *Mohamed buzubar, la criminalité informatique sur l'internet, jornal of law,n:01,année26,mars2002,university of kuweit.*
- *Redouane Semlali, Cybercriminalité :menaces et contre-mesures , Digital Maghreb, Maroc, N :4, fevrier-mars2013.*

3-Codes :

- *Code pénal français.*
- *Code de procédure pénal français.*

4-Documents :

- *conseil de l'Europe, comité des ministères, Recommandation n : R (89)9 sur la criminalité en relation avec l'ordinateur, Strasbourg, 1989, p53.*

فهرس الموضوعات

تم بعون الله

ملخص

أدي التطور التكنولوجي المذهل في مجال صناعة الحوسبة والاتصال، إلى بروز عالم تقنية المعلومات، وهي تمسّ كافة أوجه النشاط الإنساني. لكن بالمقابل نتج عن إساءة استخدامها جرائم مستحدثة تسمى: "بالجرائم الإلكترونية"، تختلف في مفهومها ووسائلها وأساليب ارتكابها عن الجرائم التقليدية. فهي جرائم تتم في بيئة رقمية عابرة للحدود ويصعب على المحققين اكتشافها وإثباتها، حيث تتسبب في أضرار نفسية واجتماعية واقتصادية بالغة، وبالتالي كان لزاما على المشرع عند وضعه لسياسته الجنائية بشقّيها الموضوعي والإجرائي، الإحاطة الشاملة بماهية هذه الجرائم المستحدثة وبكافة أشكالها قصد تحقيق الفعالية في مكافحتها، وضمان لعدم إفلات المجرم الإلكتروني من العقاب.

في هذا الشأن، سارع المشرّع إلى تعديل قانون العقوبات بتجريم الاعتداءات على شرف واعتبار الأشخاص باستعمال أي وسيلة إلكترونية بموجب المواد:(144مكرر-144مكرر2)، إضافة إلى تجريم المساس بحرمة الحياة الخاصة للأفراد باستعمال الوسائل التقنية بموجب المواد من: (303مكرر-303مكرر3). وفي المجال نفسه، قام المشرع بتعديل قانون العقوبات مرة أخرى بموجب القانون رقم: 04-15 المؤرخ في: 2004/11/10 بإضافة قسم سابع مكرّر عنوانه:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات" المواد:(394 مكرر- 394 مكرر7)، حيث كان يهدف إلى حماية نظام المعالجة الآلية للمعطيات. وباعتبار عدم كفاية الإجراءات التقليدية لكشف الجرائم الإلكترونية بسبب طبيعتها الخاصة سارع المشرّع إلى تعديل قانون الإجراءات الجزائية بموجب القانون رقم:06-22 المؤرخ في: 2006/12/22 ، أين نصّ على أساليب خاصة للبحث والتحري تتلائم وطبيعة هذه الجرائم المستحدثة وذلك بموجب المواد:(65 مكرر5 -65 مكرر18)، كاعتراض المراسلات وتسجيل الأصوات...إلخ.

كما نصّ القانون رقم:09-04 المؤرخ في:2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على جملة من الإجراءات الوقائية كمراقبة الاتصالات الإلكترونية، حيث كان هدف المشرع الوقاية من الجريمة قبل حدوثها.

ونظرا للبعد الدولي للجرائم الإلكترونية، صادقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ:2014/09/08، والتي تنص على جرائم جديدة كالتزوير الإلكتروني والإباحية الإلكترونية، إضافة إلى عقد اتفاقيات ثنائية في هذا المجال. وفي الصدد نفسه، أصدر المشرع القانون رقم:15-04 المؤرخ في:2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين أين نص على عقوبات جزائية وإدارية في حالة اساءة استخدام هذه التقنية، بما يمكّن المشرّع في

الأخير من تدارك التأخر في هذا المجال، ووضع سياسة جنائية فعّالة ومتكاملة لمكافحة الجرائم الإلكترونية.

Résumé

Le développement technologique étonnant dans l'industrie des communications et de l'informatique, a conduit à l'émergence du monde de la technologie de l'information, qui affecte tous les aspects de l'activité humaine.

Mais en échange, l'utilisation abusive de cette technologie a entrainé de nouveaux crimes appelés « la cybercriminalité » qui diffère dans leur concept et des moyens et des méthodes de commettre des crimes traditionnels.

Ce sont des crimes commis dans un environnement numérique sans frontalière, d'où les enquêteurs trouvent d'énormes difficultés pour les détecter et les prouver.

La cybercriminalité provoque des dommages psychique et social et économique, c'est ainsi que le législateur, avant de promulguer une politique criminelle de fond et de procédure, doit avoir une large connaissance de ces crimes connus récemment et de toutes ces formes afin d'atteindre une lutte efficace contre ces crimes et assurer une lutte contre l'impunité du criminel informatique.

À cet égard, le législateur Algérien n'a pas tardé à modifier le Code pénal en criminalisant les attaques sur outrages et violence à fonctionnaire et institutions de l'État en utilisant des moyens électroniques en vertu des articles: (144 bis -144 bis 2), en plus la criminalisation des atteintes portées à la vie privée des personnes en utilisant des moyens techniques en vertu des articles: (303 bis -303 bis 3).

Et Dans le même sens, le législateur a modifier de nouveau le code pénal en vertu de la loi n °: 04-15 daté du: 10/11/2004 en y ajoutant une septième division bis intitulé " des atteintes au système de traitement automatique de données" , articles :(394 bis- 394 bis7),ou le but était de protéger le systèmes de traitement automatisés de données.

Compte tenu de l'insuffisance des procédures traditionnelles pour découvrir la cybercriminalité en raison de leur nature particulière, le législateur s'est dépêché pour modifier le Code de procédure pénale en vertu de la loi n °: 06-22 daté du: 22/12/2006, en introduisant des méthodes spécifiques concernant la recherche et l'investigation adaptées à ces nouveaux crimes en vertu des articles (65 bis 5 - 65 bis 18), comme "l'interception de correspondances, des sonorisations et des fixations d'images…etc".

Dans la même optique, la loi n °: 09-04, daté du :05/08/2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication, a mis un ensemble de procédures pénales tel que"la Surveillance des communications électroniques", Ou l'objectif du législateur était de prévenir le crime avant qu'il ne survienne.

En raison de la dimension internationale de la cybercriminalité, l'Algérie a ratifié "la Convention arabe pour la lutte contre la cybercriminalité", en date du : 08/09/2014 qui prévoit de nouveaux crimes tel que : "l'infraction de falsification, infraction de pornographie", ainsi que des accords bilatéraux tenus dans ce domaine.

Dans le même cadre, le législateur a adopté la loi n °: 15-04, daté du: 02/01/2015 fixant les règles générales relatives à la signature et la certification électroniques, ou il fixe des sanctions pénales et administratives en cas de mauvaise utilisation de cette technologie, permettant ainsi au législateur de rattraper le retard dans ce domaine et l'adaptation d'une politique pénale efficace et intégrée pour lutter contre la cybercriminalité.

View publication stats